



# Order and Trade Download Service Guide

2024  
Version 1.3

# Contents

1.	Introduction	3
1.1.	Audience .....	3
1.2.	Version History.....	3
2.	Order Download Service (ODS)	4
2.1.	ODS Overview .....	4
2.2.	ODS Specification .....	6
3.	Trade Download Service (TDS)	10
3.1.	TDS Overview .....	10
3.2.	TDS Specification.....	13
4.	SFTP Service	19
4.1.	SFTP Service Overview .....	19
4.2.	Connectivity .....	19
4.3.	Authentication SSH Key Usage .....	20
4.4.	Accessing the Files And Decrypting .....	23
5.	FAQ	28
6.	Appendix	31
6.1.	Appendix A – ODS & TDS File Examples .....	31

## 1. Introduction

This document details the file specifications, use cases and technical connectivity requirements, for the ASX Order Download Service (ODS) and Trade Download Service (TDS).

The intention of the ODS and TDS service is to provide Trading Participants with an alternative method of validating order and trade data in the event that existing ASX Trade protocols are not available.

The ODS and TDS is an SFTP facility, which Trading Participants can access to download their respective private order and trade files. Participant order and trade files will be generated in the event of a major ASX Trade incident and under specific circumstances when possible to do so (refer sections 2.1.3 and 3.1.3), in order to provide participants with a definitive list of all executed trades and on-book orders to support customer reconciliation activities in a major incident scenario.

The ODS and TDS extracts trades and orders direct from ASX Trade platform source processes, which are unlikely to be impacted by issues affecting components further 'downstream'. For both orders and trades lists, a file will be generated for each combination of ASX Trade Participant ID ("PID") and partition (currently four). E.g. one order file per ASX Trade Participant ID per partition and one trade file per ASX Trade Participant ID per partition.

Although order and trade file generation for the current trading day will only be available during a major incident scenario, in order to allow customers to validate both their connectivity and their ability to download and decrypt the files, a daily trade file set will be made available to each customer each morning via the SFTP service containing their previous day's trades.

### 1.1. Audience

The information contained in the document is for ASX customers wishing to connect to the ODS and TDS production and test SFTP instances, to download TDS and ODS files to support their reconciliation activities.

### 1.2. Version History

Version	Date	Comment
1.0	October 2023	Initial Version
1.1	December 2023	Minor updates to FAQ and SFTP Service sections
1.2	February 2024	ODS file duplicate 'market' header renamed to 'seriesMarket'
1.3	April 2024	Update to 4.4 Accessing the Files and Decrypting

## 2. Order Download Service (ODS)

### 2.1. ODS Overview

The ODS is designed to enable customers to obtain a definitive list of their on-book orders and the status of those orders during a major ASX Trade incident scenario. When invoked, the ODS service will generate one order file for each combination of ASX Trade Participant ID (“PID”) and partition. ODS files will then be made available on SFTP servers in both the primary and secondary ASX data centres.

ODS files are sourced direct from the ASX Trade matching engine processes, which have historically not been impacted during outages. As the service directly accesses the ASX Trade matching engine, executing this service outside of an incident would affect the performance of the ASX Trade platform. Due to this impact, the ODS will only ever be available in a major incident scenario, and will not be available during normal operations.

#### 2.1.1 ODS File Content

An ODS file will contain order records when the ASX Trade matching engine is available and the PID has orders in that partition.

ODS files are generated in CSV format and contain a full set of order detail fields that closely mirror those found within ASX order management and information dissemination protocols, to support the ability for customers to programmatically ingest ODS files, if they choose to do so.

ODS files will contain order records for:

- orders from TradeMatch
- orders from Centre Point Order Book
- trade reports (unmatched single-sided)
- dual-posted orders (two identical order records will be generated, one for each TradeMatch and Centre Point order book orders)
- quotes

ODS files will contain no order records, and only header and footer rows when:

- the partition is available but the PID has no orders in that partition
- the partition is impacted and, as a result, there are no orders in that partition

**Note:** ASX Participants using the ODS should be capable of handling ODS files with zero order records.

All at-rest ODS files will be encrypted with a randomly generated key and must be decrypted before use, see sections 4.1 and 4.4 for further details on this process.

#### 2.1.2 Validity of Orders

When the ODS is available, both non-zero and zero order record files can be taken as a definitive and correct statement of the orders present in ASX Trade.

### 2.1.3 ODS File Availability

ODS files will only be generated and made available if a major incident occurs on the ASX Trade platform and these conditions are true:

- The market is in the ENQUIRE session state
- ASX has confirmed it will not be re-opening the market that day
- Order data cannot be accessed via the normal protocols
- The ODS data source is not impacted by the incident

ODS files will be placed on ASX's SFTP site in a directory which is accessible only by the respective Participant's authorised SFTP login and key.

ASX will inform Participants that the ODS files are available via an update to ASX's System Status Page (SSP).

### 2.1.4 ODS File Location and Naming Convention

When generated, ODS files will be placed in the home directory for each respective participant on the ASX SFTP servers.

ODS files will be named according to the following file naming convention:

[PID]\_p[partition]\_[tradedate-YYYYMMDD]\_orders.csv.enc

The following example lists four orders files within the home directory for Participant 551:

- /551\_p1\_20230816\_orders.csv.enc
- /551\_p2\_20230816\_orders.csv.enc
- /551\_p3\_20230816\_orders.csv.enc
- /551\_p4\_20230816\_orders.csv.enc

## 2.2. ODS Specification

### 2.2.1 ODS Message Format

ODS Files will be in CSV format. Sample ODS files are available, please see Appendix 6.1.

The following is true for all ODS files:

- Numeric, Length is size of field in bytes in the native protocol, however any numeric is displayed as plain text
- For Alpha fields, Length corresponds to the number of characters in the field
- Text and alpha fields may or may not be space padded and could be empty, dependent on the protocol
- The **exchangeinfo** field can contain data that is not printable. A character will only be printed if it is between 32 and 126 (ASCII decimal), if it is outside that range it will be replaced with a space. However, the content of the field should not have any impact on the ability to identify or act on the order

Field Name	Length	Value	Description
book	32	Alpha	Orderbook/Security Name.
bidOrAsk	1	Alpha/Byte	The type of order being entered: 1 = Buy order 2 = Sell order 0 = Undefined.
qty	8	Numeric/Long	Order Quantity.
premium	8	Numeric/Long	Price.
orderNr	17	Alpha	Order number. Displayed as hex.
customerInfo	15	Alpha	Free text pass through. Customer information – a free text field typically used by the customer to indicate their own order identifier.
clientOrderId	15	Alpha	Unique identifier set by the client. Currently only used in the OUCH protocol.
exClient	10	Alpha	A free text field typically used by the customer to indicate the ultimate client making the order.
pid	5	Alpha	Owner participant id of the order.
userId	5	Alpha	Owner user id of the order.
market	1	Numeric	Market of the order.
clearer	5	Alpha	Clearing identifier
exchangeOrderType	2	Numeric	0=Undefined 1=Force 2=ShortSell 4=MarketBid 8=PriceStabilization 16=OverrideCrossing 32=UndisclosedQuantityOrder 64=CentrePointOrder 128-

			8=AlwaysInactive 256=CentrePointCrossing 512=TriggerOnSession 1024=PegOrder 2048=CentrePointSweepOrder 4096=CentrePointBlockOrder Note: this is a bitmask field e.g. 2048+2 = CentrePointSweepOrder+ShortSell
leavesQty	8	Numeric	Leaves quantity.
timeValidity	2	Numeric	Defines the validity period for an order transaction, i.e. the amount of time an order will remain in the order book if not fully matched, cancelled or purged: 0=Bouncing (FoK/FaK) 1=Day Only 2=Good for Expiry 5=Good for Day 6=Good Till Cancel 32=Good Till Session.
timeS	4	Numeric	Timestamp in seconds.
timeNS	4	Numeric	Timestamp in nano seconds.
bookid	4	Numeric	Id of the order book.
ownerName	5	Alpha	User name of the order owner.
block	4	Numeric	Block size. When timeValidity = 0, this field denoted FoK or FaK. E.g. Fill Or Kill when block= 0. Fill And Kill when block = 1.
orderType	1	Numeric	0=Undefined 1=Order 2=Semi Quote 4=Price Quote 8=Bait 16=Combination 32=Trade Report 64=Crossing Order.
rankingTime	8	Numeric	Timestamp in epoch-nanosecond.
countryId	2	Alpha	Originator trading country id.
exCustomer	5	Alpha	Originator trading customer id.
country	1	Numeric	Field makes up part of the binary series definition. Country Number.
seriesMarket	1	Numeric	Field makes up part of the binary series definition. Market Code.
instrumentGroup	1	Numeric	Field makes up part of the binary series definition. Instrument Group.
modifier	1	Numeric	Field makes up part of the binary series definition. Modifier.
commodity	2	Numeric	Field makes up part of the binary series definition. Commodity Code.
expDate	2	Numeric	Field makes up part of the binary series definition. Expiration date of financial instrument. A bit pattern is used. The seven most significant bits are used for year, the next four

			<p>for month and the five least significant bits for day. All these bits make up an unsigned word. The year field starts counting from 1990. Thus, 1990=1, 1991=2 ... 2001=12.</p> <p>Example: January 1, 1990: Binary: 0000001 0001 00001 year month day 7 bits 4 bits 5 bits. Decimal: 745.</p>
strikePrice	4	Numeric	<p>Field makes up part of the binary series definition.</p> <p>The Strike Price is a part of the binary Series for options. If the Strike Price is equal to zero, it implies that the Strike Price is not applicable. This is always an integer. The implicit number of decimals is given in the decimals, strike price field.</p>
openClose	1	Numeric	<p>Open Close request:</p> <p>0=DefaultForAccount 1=Open 2=CloseNet</p> <p>3=MaandatoryClose 4=SetToDefaultForAccount.</p>
extState	1	Numeric	<p>Trade Report Type:</p> <p>0=Not applicable 1=Holding 2=Active 253=TM report cancelled by exchange 254=TM report cancelled by own customer 255=TM report cancelled by owner.</p>
stopCondition	1	Numeric	<p>Stop Condition:</p> <p>0=Undefined 1=BidLargerOrEqual 2=BidLessOrEqual</p> <p>3=OfferLargerOrEqual 4=OfferLessOrEqual</p> <p>5=LastPaidLargerOrEqual 6=LastPaidLessOrEqual.</p>
tradeReportInfo	16	Alpha	Trade report info.
boqList	6	Alpha	Basis of Quotation.
initialTradeReport	1	Numeric	Initial Trade Report: 0 = No Trade Report, 1 = yes, 2 = no.
extendedPrice	8	Numeric	Extended Price.
giveUp_countryId	2	Alpha	Giveup member country id.
settlementDate	8	Alpha	Trade Report settlement date. Date in YYYYMMDD.
timeOfAgreementDate	8	Alpha	Time of agreement date part. Date in YYYYMMDD.
timeOfAgreementTime	6	Alpha	Time of agreement time part. Time in HHMMSS.
deferredPublication	1	Numeric	1=Yes 2=No.
regulatoryData	44	Alpha	Free text pass through. Regulatory Data.
shortSellQty	8	Numeric	Short Sell Quantity.
tradeShortSellQty	8	Numeric	Short Sell Quantity - Leaves Quantity. If no value, 0 is set.
displayQty	8	Numeric	Display Quantity.



inactive	1	Numeric	Inactive status of the order: 0=No 1=Yes 2=No.
cp_minimumQty	8	Numeric	Centre point minimum quantity.
cp_midTick	1	Numeric	Centre point mid tick: 0=Off 1=Yes 2=Off 3=Dark execution 4=Dark execution with mid tick 5=Any price block execution 6=Any price block execution with mid tick.
cp_prefOnly	1	Numeric	Centre point preference only: 0=Undefined 1=Yes 2=No.
cp_singleFillMinQty	1	Numeric	Centre point single fill minimum quantity: 0=Undefined 1=Yes 2=No.
cp_participantOrderAttr	4	Numeric	Centre point participant order attributes.
cp_counterOrderAttr	4	Numeric	Centre point counter order attributes.
crossingKey	4	Numeric	Crossing key.

*Sample ODS file is available, please see Appendix 6.1*

### 3. Trade Download Service (TDS)

#### 3.1. TDS Overview

The TDS is designed to enable customers to obtain a definitive list of their executed and cancelled trades during a major ASX Trade incident scenario. When invoked, the TDS service will generate one trade file for each combination of ASX Trade Participant ID ("PID") and partition. TDS files will then be made available on SFTP servers in both the primary and secondary ASX data centres.

The ASX can source and generate TDS files from two separate ASX Trade components which are responsible for storing and disseminating trades to clearing and/or OAPI customers. Current trading day TDS files will only be generated and made available in a major incident scenario, and will not be available during normal operations.

Previous trading day TDS files will be generated and made available on a daily basis. This set of previous trading day TDS files is for TDS service validation purposes and will be made available for download by participants via the SFTP service each morning at approximately 04:00am and will contain the previous day's trades and any trade cancellations for the respective participant PID.

##### 3.1.1 TDS File Content

A TDS file will contain trade records when the Trade Handler is available and the PID has trades and/or trade cancellations in that partition.

TDS trade records contain a full set of fields that closely mirror the fields found within all ASX order management and information dissemination protocols, to support the ability for customers to programmatically ingest them, if they choose to do so.

TDS files will contain trade records for:

- executions on the current business day;
- trade reports on the current business day;
- cancellations on the current business day; and
- reports of FSSBSC (Facilitated Specified Size Block Special Crossings) trades including:
  - initial trade reports received on the previous business day where the corresponding delayed trade report was unpublished at the start of the current business day;
  - initial trade reports received on the current business day;
  - delayed trade reports published on the current business day.

TDS files will contain no trade records, and only header and footer rows when the PID has no trades or trade cancellations in that partition.

**Note:** ASX Participants using the TDS should be capable of handling TDS files with zero trade records.

All at-rest TDS files will be encrypted with a randomly generated key and must be decrypted before use, see sections 4.1 and 4.4 for further details on this process.

### 3.1.2 Validity of Trades

In a major incident scenario *matching the criteria in 3.1.3 (TDS file Availability)*, ASX will generate an initial TDS trade file as soon as it is practical to do so. ASX is statutorily obligated to take any action it considers necessary to ensure the market is fair, orderly and transparent (FOT). During incident management, ASX is guided by this overriding FOT obligation and will therefore conduct a FOT assessment to determine whether any executed trades are required to be cancelled to maintain this obligation. After completion of a FOT assessment, ASX will generate a subsequent TDS trade file set.

The initial pre-FOT assessment trade file set, generated prior to the completion of a FOT assessment, will contain an indicative view of all trades for the current trading day, including any trades under FOT assessment. Typically, all trades occurring from the start time of the incident will be subject to a FOT assessment.

The subsequent post-FOT assessment trade file set, generated after the completion of a FOT assessment, will contain a definitive view of all trades for the current trading day, and will indicate where any trades have been cancelled as a result of the FOT assessment.

Details on how the validity of trades is indicated within each file is shown in the following sections.

#### PRE FOT assessment files

Pre FOT assessment files will include an *"isValidTrade"* field. There are two possible values for this field within this file set, detailed as follows:

- "T" - indicates the trade or trade cancel stands
- "?" - indicates the trade is under FOT review

#### POST FOT assessment files

Post FOT assessment files will also include an *"isValidTrade"* field. There are two possible values for this field within this file set, detailed as follows:

- "T" - indicates the trade or trade cancel stands
- "F" - indicates the trade will not stand and may be cancelled in ASX Trade and/or in the clearing system

**Note:** trade cancellations will always be marked as 'T', meaning the trade cancellation stands.

**Note:** The *isValidTrade* field is not sourced from the trading platform and is generated and appended to each record during post-processing activity.

### 3.1.3 TDS File Availability

TDS files will only be generated and made available for the current trading day if a major incident occurs on the ASX Trade platform and these conditions are true;

- The market is in the ENQUIRE session state
- Trade data cannot be accessed via the normal protocols or disseminated trade data was erroneous
- The TDS data source is not impacted by the incident

TDS files will be placed on ASX's SFTP site in a directory which is accessible only by the respective Participant's authorised SFTP login and key.

ASX will inform ASX Participants that the TDS files are available via an update to ASX's SSP.

ASX will also generate previous trading day TDS files on a daily basis. This set of TDS files is for TDS service validation purposes and will be made available for download by participants via the SFTP service each morning at approximately 04:00am. This set of TDS files will contain the previous day's trades and any trade cancellations for the respective participant PID and partition.

### 3.1.4 TDS File Location and Naming Convention

When generated, TDS files will be placed in the home directory for each respective participant on the ASX SFTP servers.

TDS files will be named according to the following file naming convention:

[PID]\_p[partition x]\_[tradedate-YYYYMMDD]\_trades\_prefot.csv.enc

[PID]\_p[partition x]\_[tradedate-YYYYMMDD]\_trades\_postfot.csv.enc

The following example lists four pre FOT trade files within the home directory for Participant 551:

- /551\_p1\_20230816\_trades\_prefot.csv.enc
- /551\_p2\_20230816\_trades\_prefot.csv.enc
- /551\_p3\_20230816\_trades\_prefot.csv.enc
- /551\_p4\_20230816\_trades\_prefot.csv.enc

The following example lists four post FOT trade files within the home directory for Participant 551:

- /551\_p1\_20230816\_trades\_postfot.csv.enc
- /551\_p2\_20230816\_trades\_postfot.csv.enc
- /551\_p3\_20230816\_trades\_postfot.csv.enc
- /551\_p4\_20230816\_trades\_postfot.csv.enc

In a scenario when more than one set of TDS files is generated, subsequently generated files will replace (overwrite) previously generated files.

## 3.2. TDS Specification

### 3.2.1 TDS Message Format

TDS Files will be provided in csv format. Sample TDS files are available, please see Appendix 6.1.

The following is true for all TDS files:

- Numeric, Length is size of field in bytes in the native protocol, however any numeric is displayed as plain text For Alpha fields, Length corresponds to the number of character in the field
- Text and alpha fields may or may not be space padded and could be empty, dependent on the protocol
- The **exchangeinfo** field can contain data that is not printable. A character will only be printed if it is between 32 and 126 (ASCII decimal), if it is outside that range it will be replaced with a space. However, the content of the field should not have any impact on the ability to identify or act on the trade

Field name	Length	Value	Description
tradeNumber	4	Numeric	An increasing sequence number assigned to each trade. Trade number is unique within Instance and Instrument type for bid side (1).
boughtOrSold	2	Numeric	Side of the trade: 1 = Bought, 2 = Sold.
securityName	32	Alpha	Human readable name of series.
orderbookId	4	Numeric	Numerical unique ID of the orderbook.
country	2	Numeric	Field makes up part of the binary series definition. Country Number.
market	2	Numeric	Field makes up part of the binary series definition. Market Code.
instrumentGroup	2	Numeric	Field makes up part of the binary series definition. Instrument Group.
modifier	2	Numeric	Field makes up part of the binary series definition. Modifier.
commodity	4	Numeric	Field makes up part of the binary series definition. Commodity Code.
expirationDate	4	Numeric	Field makes up part of the binary series definition. Expiration date of financial instrument. A bit pattern is used. The seven most significant bits are used for year, the next four for month and the five least significant bits for day. All these bits make up an unsigned word. The year-field starts counting from 1990. Thus, 1990=1, 1991=2 ... 2001=12.

strikePrice	4	Numeric	Field makes up part of the binary series definition. The Strike Price is a part of the binary Series for options. If the Strike Price is equal to zero, it implies that the Strike Price is not applicable. This is always an integer. The implicit number of decimals is given in the decimals, strike price field.
dealPrice	4	Numeric	Deal price.
tradeQty	8	Numeric	Number of contracts in deal.
tsn	4	Numeric	Trade slip number, a unique identifier per deal. Format is 0DINNNNNNN where: 0 = Always 1, D = last digit of date calculated as number of days since 1/1 (1st of Jan) up to current business date + 50 MOD 10, I = running instance of server, NNNNNNN = running number of deal (resets to 000001 every new business day). In installations using Trade slip number, this number will be equal to the value found in External Clearinghouse Sequence Number.
ownerExCustomer	5	Alpha	This field together with Country Name, identifies a member/participant of the exchange that is the owner of this trade.
clearerId	5	Alpha	Clearer identifier for the participant of this trade.
ownerUserId	5	Alpha	ID for the owning user of this trade within the owning member specified in ownerExCustomer.
customerInfo	15	Alpha	Free text pass through. Customer information – a free text field typically used by the customer to indicate their own order identifier.
orderId	17	Alpha	Order number. Displayed as hex.
dealSource	2	Numeric	Deal source. See table deal_source_c in OAPI spec for details on values.
extTState	2	Numeric	Defines the trade report code used. 0 indicates system matching.
tradeCondition	4	Numeric	The condition in which a trade was executed. See table trade_condition_c in OAPI spec for details.
exchOrderType	4	Numeric	Bit-coded field for exchange specific order types and attributes. See exch_order_type_n table in OAPI spec for details.
tradeType	2	Numeric	Indicates what type of trade this is: 0 = Undefined 1 = Normal, 4 = Reversed / Cancelled.

accountId	10	Alpha	A free text field typically used by the customer to indicate the ultimate client making the order.
openCloseReq	2	Numeric	Describes how the requested position account should be updated: See table open_close_req_c in OAPI spec for details on values.
leState	2	Numeric	Always set to 4.
onBehalfCountry	2	Alpha	Country of OnBehalfOf participant.
onBehalfExCustomer	5	Alpha	Participant name of OnBehalfOf participant.
onBehalfUserId	5	Alpha	User ID of OnBehalfOf user in OnBehalfOf participant.
asOfTimeDate	8	Alpha	As of date for trade in local time. Date in YYYYMMDD.
asOfTimeTime	6	Alpha	As of time for trade in local time. Time in HHMMSS.
modifiedTimeDate	8	Alpha	Modified date for trade in local time. Date in YYYYMMDD.
modifiedTimeTime	6	Alpha	Modified time for trade in local time. Time in HHMMSS.
originalTradeNumber	4	Numeric	The original trade number for the cancelled trade.
createdTimeDate	8	Alpha	Created date for cancelled trades otherwise created date in local time. Date in YYYYMMDD.
createdTimeTime	6	Alpha	Created time for cancelled trades otherwise created time in local time. Time in HHMMSS.
executionTimeS	4	Numeric	Created date for cancelled trades otherwise execution date in local time. In epoch seconds.
executionTimeNS	4	Numeric	Created time for cancelled trades otherwise execution time in local time. Is the nano second component.
tradeState	1	Numeric	Trade state: 1 = Active, 2 = Rectified, 3 = Deferred, 4 = Transferred.
attention	1	Numeric	Always set to "0".

dealNo	4	Numeric	A number that identifies a specific deal. Deal number is unique within Instance and Instrument type.
globalDealNo	1	Numeric	Always set to "0".
exchangeInfo	32	Alpha	An exchange specific field and can be used for different purposes, e.g. as a free text field or trade report information.
bigAttention	8	Numeric	The field big_attention gives information about the trade for side 1. This is a bit field that gives the following information, where the first bit is bit 0, and the value column represents each bit's numerical value. Note that not every value is applicable for every installation. For details on values see table big_attention_u in OAPI spec.
clearingDate	8	Alpha	Clearing date of trade. Date in YYYYMMDD.
tradingVenue	1	Numeric	Always set to one "1".
counterPartyCountry	2	Alpha	Country of counter party participant.
counterPartyExCustomer	5	Alpha	Participant name of counter party participant.
executionEvent	17	Alpha	An ever increasing number per partition, assigned to an execution event.
matchGroup	4	Numeric	A sequential number of an execution sequence number.
matchItem	4	Numeric	Match item number inside a match group number.
ownerCountry	2	Alpha	Country of owner participant.
giveUpCountry	2	Alpha	Country of give up participant.
settlementDate	8	Alpha	Settlement date for delivery or payment. Format YYYYMMDD.
counterPartyCapacity	1	Alpha	If a trade is a cross, publishes the opposing orders Agent Capacity.
tradeReportAttribute	1	Numeric	Trade report attribute: 0 = No Trade Report, 1 = Initial trade report, 2 = Trade Report.
extendedPrice	8	Numeric	Extended price.
as_of_date	8	Alpha	The date an object is valid for. Date in YYYYMMDD.
regulatoryData	44	Alpha	Free text pass through. The regulatory data required to be submitted with orders and trade reports.
comboCountry	2	Numeric	Country and exchange identity. Country Number is a part of the Series definition.



			Combo fields are only present on the first equity leg of a TMC that also includes derivative legs, otherwise they are zero.
comboMarket	2	Numeric	<p>Binary Description representation of the market. Unique together with country.</p> <p>Combo fields are only present on the first equity leg of a TMC that also includes derivative legs, otherwise they are zero.</p>
comboInstrumentGroup	2	Numeric	<p>A unique binary representation of the instrument group.</p> <p>Combo fields are only present on the first equity leg of a TMC that also includes derivative legs, otherwise they are zero.</p>
comboModifier	2	Numeric	<p>Expiration date modifier. This value is set to zero when the instrument is new. The value is incremented by one each time the instrument is involved in an issue, split, etc. Note that the modifier value can be different for bid and ask options in the same Series.</p> <p>Combo fields are only present on the first equity leg of a TMC that also includes derivative legs, otherwise they are zero.</p>
comboCommodity	4	Numeric	<p>Underlying definitions are defined by each exchange. Commodity Code is a part of the Series definition.</p> <p>Combo fields are only present on the first equity leg of a TMC that also includes derivative legs, otherwise they are zero.</p>
comboExpirationDate	4	Numeric	<p>Expiration date of financial instrument. A bit pattern is used. The seven most significant bits are used for year, the next four for month and the five least significant bits for day. All these bits make up an unsigned word. The year-field starts counting from 1990. Thus, 1990=1, 1991=2 ... 2001=12.</p> <p>Combo fields are only present on the first equity leg of a TMC that also includes derivative legs, otherwise they are zero.</p>
comboStrikePrice	4	Numeric	<p>The Strike Price is a part of the binary Series for options. If the Strike Price is equal to zero, it implies that the Strike Price is not applicable. This is always an integer. The implicit number of decimals is given in the decimals, strike price field.</p> <p>Combo fields are only present on the first equity leg of a TMC that also includes derivative legs, otherwise they are zero.</p>
shortSellQty	8	Numeric	Short Sell Quantity.
isValidTrade		Alpha	<p>'T' = trades are deemed valid.</p> <p>Any user or exchange initiated trade cancellation will be flagged as 'T' (True).</p>

			<p>'F' = indicates the trade will not stand and may be cancelled in ASX Trade and/or in the clearing system.</p> <p>'?' = under FOT assessment</p> <p>Note: Refer to 'Validity of Trades' section in this document for further information.</p>
--	--	--	---

*Sample TDS files are available, please see Appendix 6.1*

## 4. SFTP Service

### 4.1. SFTP Service Overview

When ODS and/or TDS files are generated, they will be made available from dedicated SFTP servers from both the ASX Primary (ALC) and Secondary (SDC) sites. Connectivity to these servers is available for co-location and ASX Net customers.

The files are encrypted with a randomly generated key, the randomly generated key will be encrypted with the customers supplied public RSA key. The corresponding private key will be required to decrypt the data key.

Customers may only connect from an allowed source IP or range. To prevent brute force attacks, and to increase security, password authentication will not be supported. All communications will be encrypted in transit via the SSH File Transfer Protocol (SFTP).

### 4.2. Connectivity

Connectivity Information for the TDS and ODS SFTP services are outlined below.

#### 4.2.1 SFTP Service IP Range

Production IP Range

Co-location ALC	Co-location SDC	ASX Net ALC*	ASX Net SDC*
203.6.253.123:2222	203.0.119.122:2222	x.x.x.x:6003	x.x.x.x:6004

\*The IP addresses on the client side of the ASX Net gateways and gateway-in-cabinet devices are configured by agreement with each customer.

CDE+ IP Range

Co-location ALC	Co-location SDC	ASX Net ALC	ASX Net SDC
203.0.119.162:2222	N/A	203.4.179.122:6003	N/A

#### 4.2.2 SFTP User

SFTP user name convention will be PID[ENV]. The example below shows logins for the ASX PID 551:

ASX Trade Environment	Login Example
Production	551PRD
CDE	551CDE
CDE+	551CDP

### 4.3. Authentication SSH Key Usage

The SFTP service utilises SSH symmetric keys for secure access. The requester (ASX Participant) generates the SSH key pair. SSH private key is retained by the requester and the public SSH key is provided to ASX. An SSH key pair can be utilised for one account only. The key type should be RSA, and bit length of at least 2048 bits. See example below.

**Note:** Password authentication is not supported.

#### 4.3.1 Generating a Unique Public and Private Key pair

Participants are responsible for generating their own keys. The following is an example only

Linux example: To generate a public and private key pair.

Change the highlighted number corresponding to your participant ID number.

```
# Generate a unique public and private key pair for the purposes of connecting to
the ODS and TDS SFTP service
# For example, where '551' is your firm's pid number, specify '551PRD' as the key
pair's name, for production usage. (The CDE and CDEPlus environment login IDs are
suffixed 'CDE' and 'CDP' respectively.)

ssh-keygen -t RSA -b 2048 -f ~/.ssh/551PRD
#Press Enter when prompted to apply no passphrase to the key pair

# The command above will produce two files (a key pair) for authentication to the
TDS and ODS SFTP Service
# - 551PRD          (private)
# - 551PRD.pub      (public)

# Finally, create a Pem formatted private key, that should remain on your server.
Used for decrypting files downloaded from TDS and ODS service
openssl rsa -in 551PRD -outform pem > ~/.ssh/551PRD.pem

# And a Pem formatted public key to send to ASX, along with 551PRD.pub
openssl rsa -in 551PRD -pubout -outform pem > ~/.ssh/551PRD.pub.pem
```

At the end of this process, you should have 4 key files as follows

Filename	Privacy	Purpose
551PRD	Private	For authentication to TDS/ODS SFTP service
551PRD.pub	Public	For authentication to TDS/ODS SFTP service, send to ASX.
551PRD.pem	Private	For decryption of files downloaded from TDS/ODS by customer
551PRD.pub.pem	Public	For encryption of files on TDS/ODS by ASX, send to ASX.

#### 4.3.2 Validating successful connection to the SFTP Service

Once ASX has advised that the SFTP setup has been completed, customers should validate that they can successfully connect to the service located at both ALC and SDC sites. For Participants utilising this service from ASX Net, customers should validate connectivity via both ports 6003 and 6004.

Linux example connecting via ASX Net ALC SFTP service:

```
# where '-i 551PRD' is your private key file corresponding to your participant id (pid) assigned by ASX.

# When connecting the first time, customers will be prompted to add the TDS and ODS SFTP host key fingerprint to
their local known hosts file, similar to the following. Enter 'yes' to continue.

sftp -P 2222 -i ~/.ssh/551PRD 551PRD@203.6.253.123

# The authenticity of host '[203.6.253.123]:2222 ([203.6.253.123]:2222)' can't
be established.

# ECDSA key fingerprint is SHA256:91Q3NXTGD7ck45AWicTP7HXW3dvWFkWaHOHBW1NHnA.
# ECDSA key fingerprint is MD5:b3:8a:49:1b:70:ed:8c:29:d7:e2:cc:2b:b8:de:41:51.

Are you sure you want to continue connecting (yes/no)? yes

# Warning: Permanently added '[203.6.253.123]:2222' (ECDSA) to the list of known
hosts.
```

Customers are reminded to consider their own backup access requirements to the TDS and ODS service, such as via SDC, and/or ASX Net gateway connectivity. ASX recommends that all paths identified as needed by a customer are tested on a regular basis to ensure successful operation.

#### 4.3.3 Troubleshooting issues

If issues are encountered during connectivity testing, please contact CTS noting the following details:

- date time (and time zone if not Sydney local) of the login attempt
- your server's source IP or ASX Net gateway name
- the target IP and port that was attempted
- any associated error message/s
- PID/Username

#### 4.4. Accessing the Files And Decrypting

The ODS TDS SFTP service can be accessed using most SFTP clients.

To access and decrypt the files, the typical workflow for the service is:

1. Login
2. Download the data encryption key file

```
${pid}.atrest.key
```

3. Unlock the data encryption key using the customer's private Pem key

```
openssl rsautl -decrypt -inkey ${keydir}/${pid}.pem -in  
${keydir}/${pid}.atrest.key.enc -out ${keydir}/${pid}.atrest.key
```

4. Download the TDS file and/or ODS file,

**NOTE:** ODS only available during a major incident, IWT or BCP test weekends

5. Decrypt the files using the encryption key

```
openssl enc -d -aes-256-cbc -in ${f} -out ${f_plain} -pass  
file:${keydir}/${pid}.atrest.key -nopad -md md5
```

6. Process the files as per each customer's own business requirements/needs e.g. as a means of reconciliation

An example of a full automation script provided below can be used as a guideline to assist with automating the authentication and download and decryption of files from the ODS/TDS SFTP servers.

#### 4.4.1 Sample Scripts for Automation

**Note:** This is a BASH shell script example only and is to be used as a guide on the process of, downloading, unlocking the encryption key and decrypting the files with that key.

```
#!/bin/bash
set -e
#Version 1.04
# This script is provided as-is. Tested under Bash v4.2. Customers are free to use and modify it as they see fit.
# The script assumes that your ssh keys have been named the same as your loginID for TDS + ODS SFTP server.
# i.e. Where SFTP LoginID = 551PRD, then your private key must be named 551PRD and the private pem version
551PRD.pem
#
# Usage: ./sftp_example_script.sh LoginID TargetIP:TargetPort
#        ./sftp_example_script.sh 551PRD 10.1.2.3:2222

pid=$1
target=$2
host_port_list=(${target//:/ })      #Split Target into array of hostname and port number
target_h=${host_port_list[0]}
target_p=${host_port_list[1]}
cipher=-aes-256-cbc
digest=md5
datadir=/d1/data/tds_ods/           #NOTE - Customers to update this path for where they wish to save the data files
to.
keydir=~/.ssh/                      #NOTE - Customers to update for where their ssh private keys are stored, if not
~/.ssh/

pid_num=${pid:0:3}                  #Extract numeric prefix of the Pid LoginID.
```



```
#create file list to do further custom processing
declare -a filelist=()

function echo_and_eval() {
    echo "executing: @"
    eval "$@"
}

echo "----- Connecting as '${pid}' into '${target_h}' on port '${target_p}' ----- " ;

echo "----- Fetching Today's data encryption key -----" ;
echo_and_eval sftp -P ${target_p} -i ${keydir}/${pid} ${pid}@${target_h}:${pid}.atrest.key.enc ${keydir}

echo "----- Fetching data files. -----" ;
echo_and_eval sftp -P ${target_p} -i ${keydir}/${pid} ${pid}@${target_h}:${pid_num}_*.csv.enc ${datadir}

echo "----- Unlocking the data encryption key -----" ;
echo_and_eval openssl rsautl -decrypt -inkey ${keydir}/${pid}.pem -in ${keydir}/${pid}.atrest.key.enc -out
${keydir}/${pid}.atrest.key

echo "----- Decrypting the Data Files -----" ;
for f in ${datadir}/${pid_num}_*.csv.enc ; do
    f_plain="${f%.*}"
    echo "----- Decrypting '$f' into '$f_plain' now -----" ;
    echo_and_eval openssl enc -d $cipher -in ${f} -out ${f_plain} -pass file:${keydir}/${pid}.atrest.key -nopad -md $digest
```

```
    echo "----- Decrypted file: $f plain -----"
    filelist+=("$f plain")
done

echo "----- File Fetch and Decryption Completed -----" ;

for f in ${filelist[*]}; do
    echo $f
    #NOTE - Customers can insert their specific processing/usage needs here
done

echo "----- All Done -----" ;
```

Save the above script as `sftp_example_script.sh`, set as executable, then use it as follows:

```
# ./sftp_example_script.sh 551PRD TargetIP:TargetPort
# For Example:
./sftp_example_script.sh 551PRD 203.6.253.123:2222

#This same script can also be used by participants that have multiple pids, such as 551 and 552, in the following
way:
for user in 551PRD 552PRD; do ./sftp_example_script.sh $user 203.6.253.123:2222 ; done
```

## 5. FAQ

### Is use of the ODS & TDS mandatory?

No, however ASX strongly recommends that all participants make use of both ODS and TDS files to support trade and order reconciliation.

### Can we use the same public key for our Test and Production accounts?

No, to ensure the control are in place, ASX require separate keys for the test and production environments.

### I want to change my public keys for accessing the SFTP server, can I do that?

Yes however, note the following caveats:

- The old public keys will be replaced by the new ones you provide to ASX.
- It is the customer's responsibility for retaining the private key and decryption key needed for any historical files. ASX will not be able to assist with any recovery of old data.

### Can I have more than 1 public key for connecting to the TDS and ODS service?

No, only 1 public key is supported at a time.

### Do you accept concurrent connections from the same or different sources?

Yes, providing the source IP address is permitted and the SSH key is valid.

### What Message Authentication Code (MAC) algorithms are permitted for the SSH key?

The following are permitted:

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- umac-128-etm@openssh.com
- umac-128@openssh.com
- hmac-sha2-512,hmac-sha2-256

### What is the max idle time?

5 minutes.

### Will my keys/logon expire?

No, login ID expiry and key age are not mandatory as part of this service.

### Do I need to download my data-at-rest encryption key each time I access the service?

Yes, the data-at-rest encryption key may change. Attempting to use an old key to decrypt files will be unsuccessful.

New data keys are regenerated with each new trading date, and remain constant for that date.

Any changes in this area, such as migration to new or stronger encryption standards, will be communicated to customers in advance, along with staging through the CDE+ testing environment for customer opportunities to test.

**What software should I use for accessing the SFTP service for downloading TDS and ODS files?**

ASX have tested using sftp (version 7.4p1) and WinSCP (version 6.1.2). Customers are free to use any software they prefer for accessing the SFTP service, but if any issues are encountered, ASX will recommend they use one of these applications.

**Can I use SCP or Rsync or FTP or protocol "XYZ"?**

No, only SFTP is supported.

**Can I use password authentication?**

No, only key-based authentication is supported.

**My participant has multiple PIDs registered under the same entity with ASX (e.g. perhaps due to participant A being acquired by participant B). Can ASX combine all my firm's data into one PID login on the SFTP site?**

No, all the order and trade data activity under a given PID number will only be accessible on the SFTP server under the same numbered PID login ID.

Customers in this situation will need to connect once under each PID they hold and collect the files applicable to each. The provided scripts in this guide are written to assist with this use case in mind.

**Can I have more than one SFTP login per PID?**

No, all customers are limited to a maximum of one SFTP login per PID.

**Do I need to set up separate SFTP private/public key pair for each PID our participant firm holds?**

Yes, for a customers that have multiple PID's, they will need to send ASX a sets of keys.

**What can I do if I am getting an error when I try to connect?**

Please contact your participants Admin Support team, and CTS in the second instance.

**Are there any sample ODS/TDS files available?**

Yes, sample ODS and TDS files are available in appendix section of this document.

**Will I need to perform a conformance test?**

No, there is no conformance testing requirement for use of the ODS/TDS service.

**Can I access the ODS/TDS service over any existing Co-Location and ASX Net services?**

Access can be configured over ASX Net, OMNet and OUCH Liquidity Cross Connect (LCC). ITCH LCC is not supported for this service.

**Do I need existing ASX Trade network connectivity to utilise the ODS/TDS service?**

Yes – Participants are required to have existing ASX Trade network connectivity (ALC Cross-Connect or ASX Net) in order to utilize the ODS/TDS service.

**Can I access to test ODS/TDS servers via production Liquidity Cross Connect (LCC) services?**

No, test access can only be configured over test LCC connections.

## 6. Appendix

### 6.1. Appendix A – ODS & TDS File Examples

Sample ODS and TDS files are available in the ASX Trade technical document library:  
<https://www.asxonline.com/public/documents/asx-trade-technical-library.html>

#### Disclaimer

This document provides general information only and may be subject to change at any time without notice. ASX Limited (ABN 98 008 624 691) and its related bodies corporate (“ASX”) makes no representation or warranty with respect to the accuracy, reliability or completeness of this information. To the extent permitted by law, ASX and its employees, officers and contractors shall not be liable for any loss or damage arising in any way, including by way of negligence, from or in connection with any information provided or omitted, or from anyone acting or refraining to act in reliance on this information. The information in this document is not a substitute for any relevant operating rules, and in the event of any inconsistency between this document and the operating rules, the operating rules prevail to the extent of the inconsistency.

#### ASX Trade Marks

The trademarks listed below are trademarks of ASX. Where a mark is indicated as registered it is registered in Australia and may also be registered in other countries. Nothing contained in this document should be construed as being any licence or right to use of any trade mark contained within the document.

ASX® Limited, ASX®, ASX Trade®, Centre Point Block®, Centre Point Order®