



Securities Services

SIX Trade Repository AG

Technical Specification

May 2017



SIX Trade Repository AG

Technical Specification



Table of contents

1.0	Introduction	4
1.1	Purpose	4
1.2	Acronyms	4
1.3	Version table	4
2.0	Overview of systems and workflows	4
3.0	Input connectivity options	6
3.1	FTS-Gateway	6
3.1.1	SFTP protocol	6
3.1.1.1	SFTP requirements	6
3.1.2	SFTP software	7
3.1.3	SFTP on Unix	7
3.1.4	SFTP on Windows	7
3.2	Manual upload via GUI	7
3.2.1	GUI Access	7
3.2.2	Certificate Management	7
3.2.3	User setup and initial login procedure	8
3.2.4	Naming convention for certificate owner name	10
3.2.5	IP access restriction	10
3.3	MQ via SIX messenger	10
4.0	Reporting specifications	10
4.1	Standard file structure	10
4.2	File naming conventions	11
4.3	Compressed files	11
4.4	File size and order processing	11
4.4.1	Character set	11
4.4.2	Alphanumeric data	11
4.4.3	Numeric data	12
4.4.4	Date and time fields	12
4.4.5	Optional and unused fields	12
4.5	Record layout / header row	12
5.0	Validation response files	13
5.1	Overview	13
5.2	Response	13
5.2.1	Response file name	13
5.2.2	Header row	14
5.2.3	Data	14
5.2.4	Footer	15
6.0	Data reports	15
6.1	Trade Repository data extract	15
6.1.1	Data content	15



SIX Trade Repository AG

Technical Specification

6.1.2	File format and name	15
7.0	Field specification	16
8.0	Validation and exception codes	16
9.0	Contact	16

SIX Trade Repository AG

Technical Specification



1.0 Introduction

1.1 Purpose

This document provides a technical overview of the SIX trade repository application (an interface for clients to manage the derivatives reporting obligations imposed by FinfraG and to deliver derivative trade reports to the SIX TR).

The information provided in this document is subject to change and update at short notice. All document updates will be shown in the version table (chapter 1.3).

1.2 Acronyms

Abbreviation	Meaning
FINMA	Swiss Financial Market Supervisory Authority
FinfraG	Swiss Financial Market Infrastructure Act (FinfraG)
FinfraV	Ordinance to the FinfraG
GUI	Web user interface of the Reporting System
SIX TR	The SIX company that will offer the trade repository service
TR	Trade Repository

1.3 Version table

Document version	Release date	Information
V1.0 (draft)	20 May 2015	First draft release, to be amended according to requirements for trade reporting in Switzerland as made available by the competent regulatory authorities.
V2.0 (draft)	19 August 2015	Added process for generation and installation of client certificates in chapter 3.2.2.
V2.1 (draft)	2 October 2015	Added details to the obfuscation of client identifying data in the SIX TR response files, updates on FTS gateway and date/time formats
V0.5	15 December 2015	Updated file naming convention omitting prefix rules (chapter 4.2 and 4.3). Updated initial login process (chapter 3.2.1.)
V0.6	06 May 2016	Added Certificate Mgmt. option with client certificate and naming conventions for certificate owners (chapter 3.2.2. – 3.2.4.)

2.0 Overview of systems and workflows

The SIX TR offering comprises two different systems: **the Reporting System** and **the Trade Repository**.

SIX Trade Repository AG

Technical Specification

The Reporting System is the client-facing part of the system. It accepts data from clients, validates it, and passes it on to the Trade Repository database.

The Trade Repository feeds back confirmation of acceptance and validation results to the Reporting System for client consumption. The Trade Repository holds a permanent record of all FinfraG reports received and presents the data to the regulator and authorities that may request it pursuant to Swiss legislation.

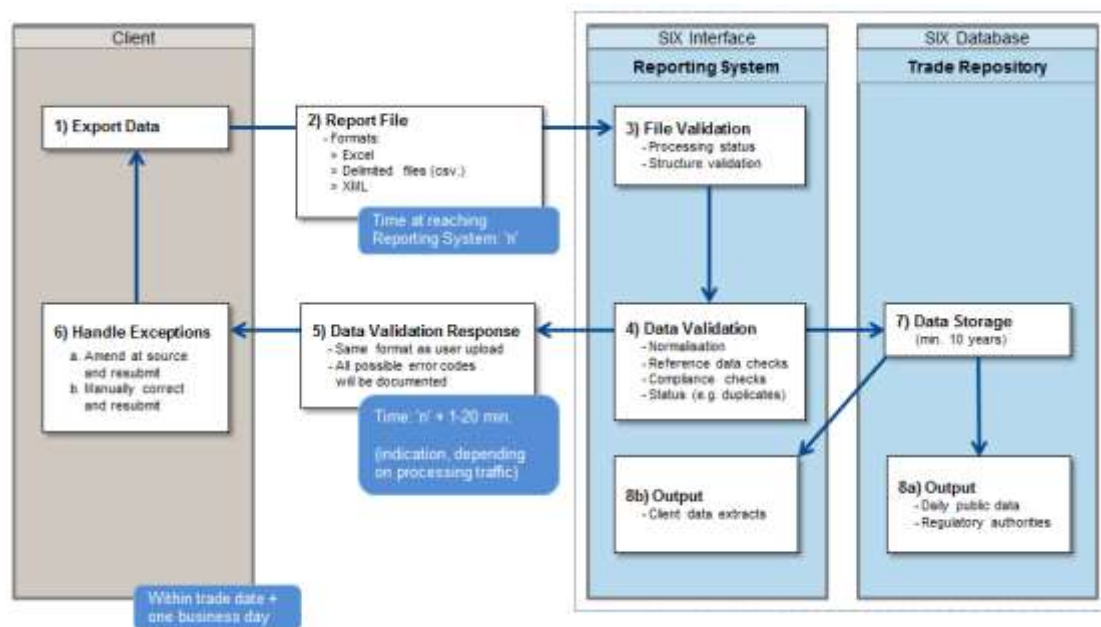


Figure 1: Overview of systems and workflows

1. Client delivers data to the Reporting System through the import function in the GUI, via file transfer Gateway (FTS) or by sending and receiving via message queues (MQ).
2. The report file is accepted in various formats (see chapter 4.1).
3. File level validation of the Report File is performed. This covers structure validation (e.g. corrupt ZIP or Excel file) and structural checks (e.g. unrecognized fields).
4. Data is validated by the Reporting System. Once data has been imported to the Reporting System, it follows a prescribed workflow that includes field length checks, data type validation, business-level validation, exception handling and report submission to the regulator (see step 7).
5. TR system sends back a data validation response. Validation processing results with exceptions are documented in a report sent to the client.
6. Client handles exceptions, either by resolving in own back end source system or through the manual GUI export process as documented in the SIX Reporting System User Guide.



SIX Trade Repository AG

Technical Specification

7. Reporting data is stored in the Trade Repository once it has been fully accepted and reporting data is then available to the regulator. The regulator may request scheduled reports.
8. Data extracts from the Trade Repository and reports are made available to the participant.

3.0 Input connectivity options

Given that the reporting obligation has to be fulfilled T+1 and not real-time, the Reporting System aims to take data in a file format, rather than single message formats. The list below is of the standard options that are expected. The Reporting System has a functionality suite for the import of files, covering timings of imports, acknowledgements, retry and deferral options.

The below transportation methods are secure and accepted:

- FTS-Gateway
- Direct upload through the Reporting System https user interface
- MQ via SIX messenger

3.1 FTS-Gateway

The FTS-Gateway is a UNIX-based file transfer platform facilitating file exchange over heterogeneous networks and enabling automatic and secure file transfer with different file transfer protocols. The FTS-Gateway offers the possibilities to push files (recommended for trade reporting) or to pull them. The focus of this chapter is on the description of the SFTP protocol.

3.1.1 SFTP protocol

The SFTP or "SSH File Transfer Protocol" is an encrypted transport protocol designed to provide secure file transfers over public networks.

3.1.1.1 SFTP requirements

A standard SFTP implementation is required. To communicate with the FTS-Gateway using the SFTP protocol, the following requirements must be fulfilled:

- Client authentication method is PublicKey
- The key type to use is RSA
- Minimum key length is 2048 bit
- Partner accounts are activated only after verifying their keys fingerprint
- Utilized encryption algorithms are AES128_CBC or 3DES_CBC
- MAC algorithms are SHA1 or MD5
- Key exchange algorithm is DH_GROUP1_SHA1



SIX Trade Repository AG

Technical Specification

3.1.2 SFTP software

To be able to exchange files over the FTS-Gateway with SFTP, a standard SFTP implementation is required. The SIX FTS competence center will work out the setup directly with the client's technical contact person. SIX and the client agree on the routing prefix information for inbound and outbound file transfer.

Prefix naming convention:

<T|P><Recip-ID>.<Orig-ID>.<File-ID>.<Appl-Info>

T P	Test or production flag (either of the values)
Recip-ID	Recipient identification
Orig-ID	Sender identification
File-ID	File-type is always 'SDTR'

The parts are separated with a full stop. No separation between <T|P> and <Recip-ID>. Recip-ID and Orig-ID are used for routing. File ID is referencing the service 'SDTR'.

3.1.3 SFTP on Unix

Unix operating systems are delivered with suitable SFTP software (OpenSSH or SSH).

3.1.4 SFTP on Windows

A variety of free and commercial SFTP client software is available. Good results have been achieved with Cygwin, a free GNU-based UNIX environment for Windows.

3.2 Manual upload via GUI

The manual uploading of files to the Reporting System via web interface is documented in the SIX Reporting System User Guide.

3.2.1 GUI Access

Interactive access to the Reporting System can be achieved over the Internet via the HTTPS protocol. In order to log on to the GUI, users need to have the appropriate credentials and access rights.

The following credentials are required to log on to the Reporting System:

- Reporting System user name (e-mail address)
- Password
- Digital certificate

3.2.2 Certificate Management

SIX TR AG provides a user certificates for authentication of each user and each environment he is setup (SIX CA).



SIX Trade Repository AG

Technical Specification

As an alternative, clients with own certification authority (client CA) can provide their root certificate information to SIX. SIX TR AG will store this information and authenticates the user accordingly. The user account information (e-mail address) is the attribute which links user public key and user account.

A client chooses either the standard SIX CA or his own client CA.

3.2.3 User setup and initial login procedure

The primary user administrator(s) will be activated by SIX during the client onboarding process based on the information defined in the Reporting User Application Form. Following first user administrator activation, additional users for the same company can be setup by the client himself.

As soon as a new user has been set up the credentials to login to the SIX PKI infrastructure will be passed to the user. From there the digital certificate can be downloaded and imported into the browser.

SIX activity	Step	Client activity
SIX client support configures user account of primary user.	1	Subsequent users will be created directly by the Client User Administrators. Mobile nr. is a mandatory information to get access to SIX CA.
The user account is activated in an over-night system process. As a result, two e-mails are sent.	2	Take the e-mail containing the URL internet link and access information for certificate download first.
	3	Use this email to request a TAN code.
A TAN code will be sent to your mobile phone (valid for a maximum of 300 seconds).	4	Authenticate yourself using the TAN code over the URL internet link.
Your certificate is available for download	5	Download the certificate using the Certificate Installation Quick Guide and install the certificate locally.
	6	Connect to the SIX Reporting System for the first time within 24 hours of creation and login with the application password sent with the second email.
The SIX TR will request that you change your initial password.	7	Change your password and log on to the SIX Reporting System.

SIX Trade Repository AG

Technical Specification

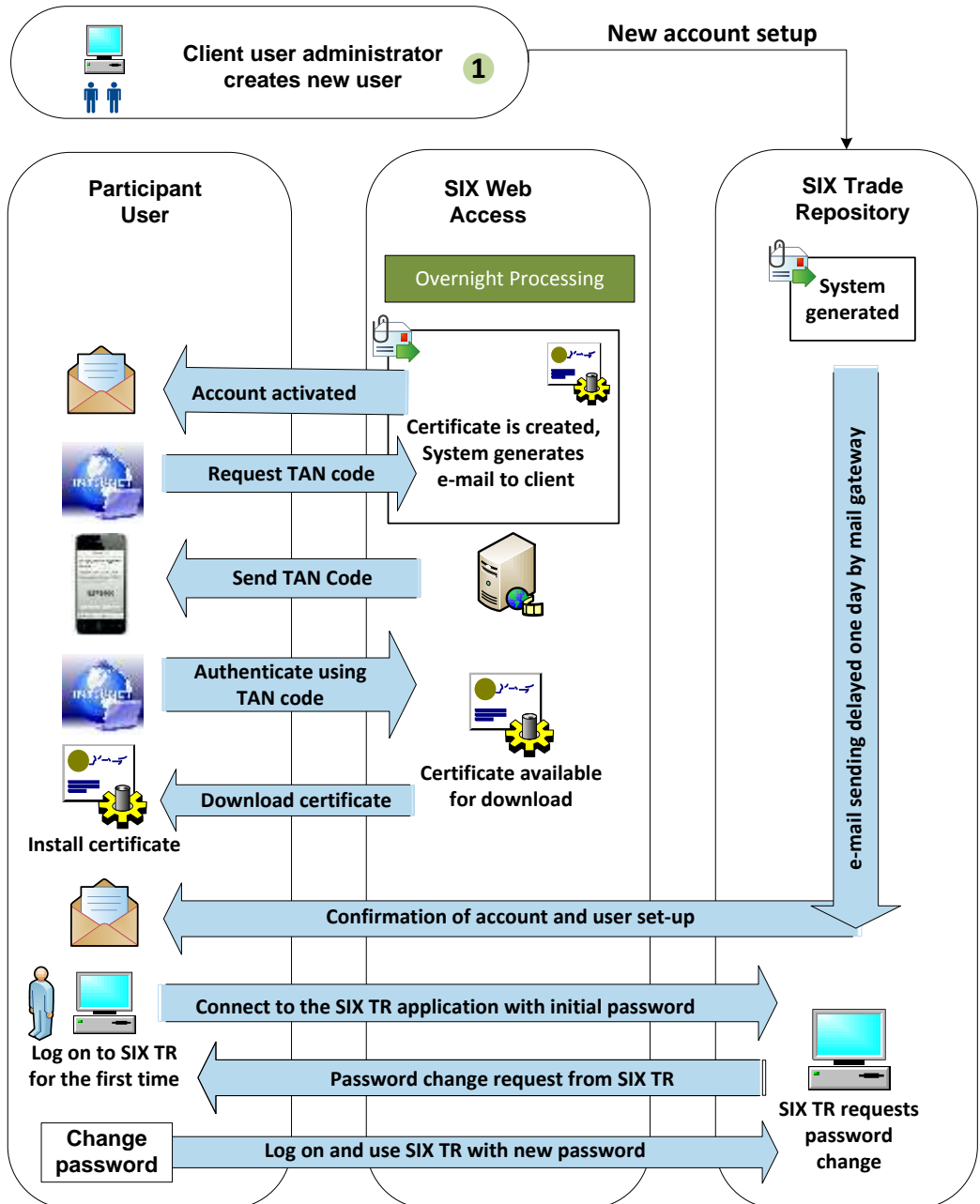


Figure 2: Process to initiate certificate download and access

The details of this process are documented in the Certificate Installation Quick Guide.

 SIX Trade Repository AG

Technical Specification

3.2.4 Naming convention for certificate owner name

The certificate owner name is derived from the user account name (prefix + email).
Certificates owner names are differentiated with a prefix:

SDTR Reporting – Member Test certificate owner name = “dtrmbt_username”
SDTR Reporting – Production certificate owner name = “dtrprd_username”

3.2.5 IP access restriction

The access to the GUI can be restricted to a defined IP address or range of IP addresses.
This is an optional feature that is documented in the SIX Reporting System User Guide.

3.3 MQ via SIX messenger

The IBM® MQ series is a robust messaging middleware that simplifies and accelerates the integration of participants to the SIX TR with a secure and high-performance exchange of information by sending and receiving message data via messaging queues. Channels are used in the context of financial institutions with an existing fixed line messaging infrastructure (e.g. Finance IP). All others are advised to use SFTP over the FTS-gateway.

4.0 Reporting specifications

This section describes the format and contents of the standard transaction reporting file required by the TR system.

The following information is included:

- the convention that firms should adopt when naming the files to be transmitted to the SIX TR
- the formats and character sets to be used when populating data fields
- the layout of records
- a description of each field contained within a record
- the fields that are required in order for the firm to meet its reporting requirements
- the validation applied to each field by SIX

4.1 Standard file structure

Below is a list of the file format that are available for submitting data to the Reporting System:

- Comma-delimited file (*.csv)
- Excel file (*.xls and *.xlsx)
- XML file

CSV-files must be delimited using the comma character “,”. Both CSV and Excel files may not be password protected. SIX provides standard templates as a guide for clients, since the use of a template reduces the risk of data corruption or incorrect data being populated.



SIX Trade Repository AG

Technical Specification

4.2 File naming conventions

Prior to the first file being loaded, the file name will need to be pre-agreed with the SIX onboarding support team. If the client requires data segregation within its own organisation (i.e. if some client users should only be able to access specific data), then multiple file naming conventions will need to be defined based on the required data segregation.

File names should not contain full stops (i.e. dots ".") other than the file extension. There are no further fixed rules regarding the naming of the file as long as the name is used consistently. We recommend the use of a file name with a date time suffix: YYYYMMDDHHmm. For example, 20151109142534 for 9 November 2015 at 14:25:34.

An example comma-delimited file name might be:

```
Firmtransactionreport_20151109142534.csv
```

4.3 Compressed files

The name of compressed files should be the data filename as above with '.zip' appended to it. For example:

```
Firmtransactionreport_20151109142534.zip
```

4.4 File size and order processing

For optimal processing, we recommend that files do not exceed 50,000 rows. For data exceeding 100,000 rows, we advise loading data in multiple files.

Files will be processed in the order that they are received by the Reporting System.

4.4.1 Character set

The files should use the 8-bit ASCII character set (ISO 8859-1). In particular:

- The end-of-record field should contain the New Line (NL) character, which is 10 in decimal (or 0A in hexadecimal);
- No other "control" or non-printable characters should be included: only ASCII characters between 32 and 127 (decimal) are permitted;
- Spaces are 32 in decimal (or 20 in hexadecimal).

4.4.2 Alphanumeric data

Alphanumeric fields are denoted by "Alpha" and may contain alpha and numeric characters.



SIX Trade Repository AG

Technical Specification

4.4.3 Numeric data

Numeric fields are denoted by "Decimal". The field length will describe the overall length and number of decimal places allowed. For example a length of 30 (25,5) allows up to and including 25 digits followed by 5 decimal places.

The decimal point must be a full stop (.) and is not counted as a numerical value.

4.4.4 Date and time fields

Date-only fields should be in the format YYYY-MM-DD.

Time fields should be in the format HH:MM:SS (24-hour clock) and can either be in UTC or Swiss local time (CEST / CEWT) depending on the chosen time format as indicated in the report.

Date and time fields should be in the ISO 8601 date and time format as elected: YYYY-MM-DDThh:mm:ss.

Each field within the date must have leading zeros where applicable. Dates must be valid. For example, 1 December 2002 would be represented as "2002-12-01".

Times must be valid. For example, 3.25 p.m. would be represented as "15:25:00", whereas 3.25 am would be represented as "03:25:00". Where firms do not have access to the seconds field for the time, they should complete the seconds with "00".

4.4.5 Optional and unused fields

Optional fields should be populated where possible. Unused fields should be left blank.

Where optional fields have been populated by the client, the values will be validated in the same way as the mandatory fields. If they pass the validation, they will be sent on to the regulator despite being optional fields.

4.5 Record layout / header row

Comma-separated and Excel files should contain a header row which contains the field names as per the Reporting Field List in correct order.

Field name
Reporting Firm ID
Other Counterparty ID Type
Other Counterparty ID
Reporting Firm Name
etc.



SIX Trade Repository AG

Technical Specification

Files should be in sequential order with older records at the top and newer records at the end.

The file content will be loaded into the Reporting System in the same order as it is in the file. In the event that the same file has dependent data rows e.g. a "New" and "Cancel" record, they should appear in the file in the following sequence:

- Header row
- New record
- Cancellation record

For the full field specification and data types, please refer to the FinfraG Reporting Field List, which is available on the SIX website: www.six-securities-services.com/derirep.

5.0 Validation response files

5.1 Overview

Response files can be generated in either pipe-delimited or XML format, as per client requirements. A response file will be produced following validation by the Reporting and Repository Systems.

Any errors returned in the validation response files are expressly for the file that was loaded. The response files are **not** cumulative and errors for that file will only be returned once. All errors will be shown in the GUI until they are resolved (either by manual action or subsequent correction). If the file is submitted again with some corrections, the validation response file will only show any errors in that latest version of the file.

For reference, please refer to the workflow diagram in chapter 2.0.

5.2 Response

The response is sent once validation has been completed on the file.

5.2.1 Response file name

Response files can be defined by SIX in pipe (|)-delimited, xml and csv file format (csv by default). The suffix “**_SIXRes.csv**” (or **_SIXRes.xml** or **_SIXRes.txt** if requested by the client) will be appended to the end.

Example:

Submitted file name	Firmtransactionreport_201511091425.csv
Response file name	Firmtransactionreport_201511091425.csv_SIXRes.csv

SIX Trade Repository AG

Technical Specification

5.2.2 Header row

Field name	Format	Description
Row Type	Integer (always 0)	0 for header row
Inbound Filename	Text (200)	Name of the file that was loaded to the SIX Reporting System
Import Date	Date/time (YYYY-MM-DDTHH:mm:ss)	Date and time that the file was received (in Swiss local time)
Reports Loaded	Integer	Number of reports contained in the file
Validation Failed	Integer	Number of reports which failed TR system validation
Validation Errors	Integer	Number of validation exceptions on reports which failed TR system validation
Reports Recorded	Integer	Number of reports recorded by the TR system

5.2.3 Data

All values in the response records are taken from the reports that were in error and so may be blank where they are blank on the report, e.g. where a client does not populate the Reporting Firm ID field on a report, the Reporting Firm ID field on the response row will be blank.

The data file will contain one row per error. For example, if on the original file row x was to contain 2 errors due to missing Reporting Firm and Counterparty data, then it would have 2 rows reporting each error and would relate both errors to row x.

Field name	Format	Description
Row Type	Integer (always 1)	1 for data row
Row Number	Integer	Position of the report within the original inbound client file
Error Field	Text (100)	Field within the report that was in error
Error Code	Integer	SIX code for the error that has occurred
Error Reason	Text (100)	English text describing the error that has occurred
Error Value	Text (200)	Data that caused the error (shows contents of error field, may be blank) Client identifying data (field "Other Counterparty ID" as per the FinfraG Reporting Field List) will by default contain the value "obfuscated".
Trade ID	Text (52)	UTI of the report (taken from the report)
Action Type	Text (1)	Action type of the report
Internal ID	Text (120)	Internal ID for usage by the reporter or submitter for internal tracking purposes



SIX Trade Repository AG

Technical Specification

5.2.4 Footer

Field name	Format	Description
Row Type	Integer (always 9)	9 for footer row
Row Count	Integer	Number of data rows in this response file, excluding header and footer
Create Date	Date/time (YYYY-MM-DDTHH:mm:ss)	Date and time that this response file was created (in Swiss local time)

6.0 Data reports

6.1 Trade Repository data extract

By using the GUI, users can request data for a Reporting Firm ID that they have submitted to the Reporting System. Files can be generated for trade or valuation data for a defined period. For information on how to request the data using the GUI, please refer to the SIX Reporting System User Guide. This section will provide details on the file format that is generated.

6.1.1 Data content

Trade and valuation data will be provided for the requested period based on the reporting timestamp. This is the timestamp of when the data row was received by the Trade Repository.

6.1.2 File format and name

The file formats are pipe (|)-delimited and csv files. All files contain a header row with the field names. The files are *.zip files that contain the *.txt or *.csv data file.

TradeDataRequest_<ReportingFirmID>_<StartDate YYYYMMdd>_{EndDate YYYYMMdd}.*{txt|csv}*.zip

ValuationDataRequest_<ReportingFirmID>_<StartDate YYYYMMdd>_{EndDate YYYYMMdd}.*{txt|csv}*.zip

For example:

- TradeDataRequest_213800QAUUUP6I445N30_20151201_20181230.zip
- TradeDataRequest_213800QAUUUP6I445N30_20151201_20181230.txt

or

- TradeDataRequest_213800QAUUUP6I445N30_20151201_20181230.zip
- TradeDataRequest_213800QAUUUP6I445N30_20151201_20181230.csv

Please note the ReportingFirmID and EndDate will be included depending on the data request made. Where the ReportingFirmID is referenced then it will also be included. If the



SIX Trade Repository AG

Technical Specification

data is for a single day, then as the start and end dates specified are the same date, the EndDate will not be included in the file name.

7.0 Field specification

The fields included in the file are fields that are stored in the Trade Repository. Some fields on the specification are used for processing purposes and may not be included on the file where they are not sent to the Trade Repository. The fields included and the data type and content are documented in the Reporting Field List: www.six-securities-services.com/derirep.

8.0 Validation and exception codes

All error codes generated by the TR system are documented and made available as part of the FinfraG Reporting Field List.

9.0 Contact

For technical questions, please contact our Service Desk. During the initial member testing phase the Service Desk can be reached via email to derirep-testsupport@six-group.com. Should you require further information of a general nature, please contact your Relationship Manager.

SIX Securities Services
Brandschenkestrasse 47
CH-8002 Zurich

Mailing address:
P.O. Box
CH-8021 Zurich

T +41 58 399 4511
F +41 58 499 4511
www.six-securities-services.com

