



SURF Feed Encryption Guide

Feed Content

Nothing in this document commits Tullett Prebon Information TPI or Tullett Prebon to supply data, or in any specific format. TPI reserves the right to withdraw supply of data without notice subject to any contractual arrangements.

Note that this feed is dependant on a core broking business working in a very dynamic market place.

TPI reserves the right to add/remove data without notice. Regular updates to the Data Content will be supplied via periodic 'Data Change Notifications'.

Related Documents

This document should be read in conjunction with the following documents:-

SURF Datasets	- a list of all data available
SURF Supporting Information	- notes giving background Market information
SURF Master Field List	- a (computer readable) list of all fields that can exist in SURF
SURF Stub Field List Stub	- a (computer readable) list of fields per Record
SURF Implementation Guide	- details of how to connect to the feed.
SURF Encryption Guide	- only supplied if required (when running live over the Internet)

Confidentiality

The information contained within this document is **confidential** and unauthorised copying or reproduction by any means is prohibited.

Ownership

TPI reserves title to, and all copyright and other intellectual property rights in this document.

Copyright © 2007 Tullett Prebon Information Ltd

Contact Details

Head Office

Tullett Prebon Information Ltd
Cable House
54-62 New Broad Street
London
EC2M 1ST

London

Sales: Tel: +44 (0) 20 7200 7600

New York

Sales: Tel: +1 877 639 7300

Support: Tel: +1 888 660 6651

Singapore

Sales: Tel: +65 6536 5843

Global Support

24 Hour Support Line* Tel: +44 (0)20 7302 5382

e-mail support@tpinformation.com

* The Global Support Line is manned 24 hours a day from 22:00 Sunday (commencement of business in Singapore) to 22:00 Friday (close of business in New York) London time.

Acknowledgements

Marketfeed™ is the property of Reuters plc.

Blowfish Cipher technology is the property of Counterpane Internet Security Inc.

E&OE

Contents

FEED CONTENT	2
RELATED DOCUMENTS	2
CONFIDENTIALITY	2
OWNERSHIP	2
CONTACT DETAILS	3
Head Office	3
Global Support	Error! Bookmark not defined.
ACKNOWLEDGEMENTS	3
CHANGE CONTROL HISTORY	5
DATA FEED DESCRIPTION	6
GENERAL COMMENTS	6
MESSAGE PROTOCOL	6
FEED INTEGRITY	7
MESSAGE FRAMING	7
ENCRYPTION	7
ENCRYPTION METHODOLOGY	8

Change Control History

Date	Version	Description
3 rd Aug 2005	6.0	Amended contact / company name details. Renumbered to move in line with other documentation
6 th Jan 2003	0.2	Amended contact details
1 st Mar 2002	0.1	First Draft

Data Feed Description

General Comments

The Tullett Prebon Information Ltd SURF (**S**imple **U**nified **R**ecord **F**eed) feed is designed to deliver Collins Stewart Tullett plc prices in a reliable and auditable form to all clients. The feed is delivered as a broadcast data stream over TCP/IP connections.

Message Protocol

SURF is heavily based on Reuters Marketfeed protocol. It is a subset of the Marketfeed protocol aimed at delivering data as simply and as efficiently as possible. It is intended that existing Marketfeed handlers will be able to read SURF with minimal alteration.

SURF outputs 4 message types consistent with Reuters Marketfeed:-

Record Type 340 – a full image record

Record Type 316 – a partial update (i.e. some fields changed)

Record Type 318 – a verify record

Record Type 407 – a status response with a code 29 'load complete'.

Each distinct record (with the exception of the status response) is identified by a unique Record Name, a 1 – 17 character field that is sent in the header of each message. The first time, the SURF system generates a new record, all the fields defined for the Record will be sent using a full image message (340). Note that the client system will potentially see most new records at logon time via 318 records (see below). 340 records will only be seen if the client is connected the very first time SURF generates the record.

When changes occur to any Record that has already been sent, only those fields that have changed will be sent to the client in a partial update record (316).

As the feed is broadcast only, there will be an optional 'periodic refresh' facility. This will send full image records to a client every 'n' seconds which the client could use to check the last update received and/or restore their CST 'dataset'. This data will be sent using a verify record (318).

In addition to the optional periodic refresh, there is an optional 'Logon Refresh'. The Logon Refresh sends all permissioned data to the connecting client via verify records (318) as quickly as possible after connection has been established. When the Logon Refresh is completed the client is sent a record type 407 with a code 29.

The time and date of the last update to a record will be reflected in the Fields 5 (format hh:mm) and 17 (format dd mmm yyyy) respectively. Any client receiving the SURF update messages (Record Type 316) should update these fields with the date and time of their own receiving system. The time will always be GMT.

Feed Integrity

As the feed is broadcast there is no way for a client to re-request or verify data. SURF utilises an update numbering mechanism so that clients can detect problems when receiving the broadcast data stream.

The data update messages (340, 316 and 318) contain a sequence number field (RTL – Record Transaction Level), which is incremented each time a Record is updated. When a client receives a 340 or 316 message the RTL field should be 1 higher than the existing value for that record.

A verify message (318) contains the current RTL value and is not incremented.

The RTL field is modulus 65535, returning to 1 (not zero)

Message Framing

In order to simplify the extraction of Marketfeed records from a data stream, each record will be preceded with four ASCII characters giving the length of the record that follow. Thus, if the Marketfeed record is 355 characters long, then the message begins with “0355”.

Encryption

If a client is taking the feed over the Public Internet in a live running mode the message will be encrypted after the message length. The receiving client feed handler will have to decrypt the message prior to decoding the Marketfeed data.

Encryption Methodology

The encryption will be based on the Blowfish cipher operating in Chained Feedback Block (Cfb64) mode. This mode operates on variable length messages without the need to pad data to a block boundary.

The Blowfish cipher was invented and described by a company called Counterpane. The specific implementation used in SURF is from the Open SSL Organisation.

TPI will supply each client with their own 16 Hex character encryption key. TPI reserves the right to change this key on an ad-hoc basis at relatively short notice, but in agreement with each Customer.

Further details of the Blowfish cipher and its implementation can be found at:-

- www.counterpane.com/blowfish.html
- www.openssl.org