Optitrade Flow

Optitrade Flow is designed to connect users’ application systems to financial networks such as SWIFT, CTM, CREST, OASYS-Domestic, FIX, etc. It supports connections via MQ, file shares, sockets, etc. and can deal with a variety of formats such as XML, csv, FLR, tag-&-value, ISO20022, 15022 etc.

It is designed to operate in a fully automatic, Straight Through Processing (STP) mode. It also has an extremely flexible Graphical User Interface that allows flows to be monitored, messages to be inspected or verified, and exceptions to be handled with speed and accuracy.

Flow Messaging

Client Security:

Internal Threats

* service denial, e.g. a malicious operator seeking to bring the system down

* data privacy, e.g. an operator gaining access to message data for financial gain

* tampering, e.g. an operator changing an outgoing message for financial gain

Security Features

* access control

* audit trails
* data validation

**External Threats**

* data privacy, i.e. an external agent reading message data

* replay attacks, i.e. an external agent repeating a message to achieve an additional payment

* tampering and repudiation, i.e. a counterparty refusing to accept that a message was produced by them and therefore repudiating a transaction giving rise to a financial loss

* contingency, i.e. loss of service due to a site disaster

**Security Features**

* data validation

* sequence numbering

* message authentication

* safestoring

**Verification and Authentication**

* Sophisticated queue management process controls preparation, amendment, validation and authentication (testing) of outbound and inbound messages.

* Typically involves at least one level of authorisation by another operator before a message can be released for transmission. It is possible to configure between zero and nine verification steps to any message process.

**Audit Trails and Message Referencing**

* Every message audit trail logs the user ID of the operator who prepares, amends, verifies, tests and transmits the message.

* Assigned a unique document reference number

* Messages are accessible to authorised users and can be tracked and retrieved by reference number, owner, sequence number, correspondent code or user-specified keywords.

**Data Validation**

* Supports an optional function known as “message checksum support”.

* Uses a **CRC-16 algorithm** stored with each body part to ensure message content is not altered outside of the access controls available within the Flow system. This mechanism provides an on screen alert in the event of any “tamper” detection. Gateways will fail the message and report an error to the Activity Log.
* Flow also supports the stronger **MD5 algorithm**. No key exchange or administration functions are required as the “key” is coded within the application.

* Where appropriate, body parts are compressed. This means that plain text is not visible to someone attempting to “tamper” with the message.

**Safe Storing**

* Flow provides a safe store in the form of a message database which can be replicated, along with other system data, to ensure that the system can be restarted from a remote location in the event of site disasters or other contingency situations.