STABILIT
Intelligente Informatik

SC

Service Connector

Requirements and Specification

SC_0_Specification_E (Version V1.8)

SC is a middleware component for new Eurex IT platform. This document summarizes the requirements, describes specifications and defines the scope of the project. It is the starting point for the design phase.

The creation of this software is sponsored by a customer. Other companies may develop similar software as a commercial product and destroy this effort in the mean time. In order to protect the investment of the sponsor and the idea of open source software, this and all subsequent documents are classified as “CONFIDENTIAL” during the development phase. They may be delivered only after signing an appropriate non-disclosure agreement. They will be published when the software development is finished and the software is made available as open source software.

During the development of this software this document is a spiritual ownership of STABILIT Informatik AG, and must not be used or copied without a written allowance of this company and signing a non-disclosure agreement. Unauthorized usage is illegal in terms of Chapter 23 / 5 UWG / Swiss law.

The information in this document is subject to change without notice and should not be construed as a commitment by STABILIT Informatik AG.

This Document has been created with Microsoft Word 2003 (11) with template file C:\STABILIT\STANDARD\TEMPLATES\S_REP_E.DOT and printed at 01 July 2010 12:02.

Identification

Project:	SC
Title:	Service Connector
Subtitle:	Requirements and Specification
Version:	V1.8
Reference:	SC_0_Specification_E
Classification:	Confidential
Keywords:	Requirements, Specification, Scope
Comment:	SC is a middleware component for new Eurex IT platform. This document summarizes the requirements, describes specifications and defines the scope of the project. It is the starting point for the design phase.
Author(s):	STABILIT Informatik AG Jan Trnka, Daniel Schmutz, Mauro Ricchetti, Joel Traber
Approval (Reviewed by):	Signature ..... Jan Trnka Signature ..... Francisco Gonzalez Signature ..... Walter Mörgeli
Audience:	Project team, Eurex IT management, Review team
Distribution:	Project team, Eurex IT management, Review team
Filename	c:\stabilit\projects\eurex\sc\documents\sc_0_specification_e.doc

Revision History

Date	Version	Author	Description
14.06.2009	D1.0	Jan Trnka	Initial draft
09.08.2009	D1.1	Jan Trnka	Separate specifications and requirements into this document and move other parts to the architecture document
25.11.2009	V1.2	Jan Trnka	Corrections from talks with SIX
20.1.2010	V1.3	Jan Trnka	Finalizing requirements
31.1.2010	V1.4	Jan Trnka	Closing open issues
7.4.2010	V1.5	Jan Trnka	Service structure better explained
22.3.2010	V1.6	Jan Trnka	Comments from SIX
2.6.2010	V1.7	Jan Trnka	Correction of multithreaded and multisession servers
17.6.2010	V1.8	Jan Trnka	SC-Proxy merged with SC.
30.6.2010	V1.9	Jan Trnka	Changes resulting from the SCMP review.

Table of Contents

Tables

Figures

1 Preface

1.1 Purpose & Scope of this Document

This document summarizes the known requirements, describes system specifications and defines the project scope.

The final and approved version of this document serves as base for the binding architecture and design, described in another document. It defines also the scope of the implementation project and is part of the contract between Eurex / SIX and Stabilit.

This document is particularly important to all project team members.

1.2 Classification

The creation of this software is sponsored by a customer. Other companies may develop similar software as a commercial product and destroy this effort in the mean time. In order to protect the investment of the sponsor and the idea of open source software, this and all subsequent documents are classified as "CONFIDENTIAL" during the development phase. They may be delivered only after signing an appropriate non-disclosure agreement. They will be published when the software development is finished and the software is made available as open source software.

1.3 Definitions & Abbreviations

Item / Term	Definition / Description
DMZ	Demilitarized Zone (Network segment between two firewalls)
DOS	Denial Of Service
EBS	Elektronische Börse Schweiz – older project name for ESY
ERM	Electronic Repo Market
ESY	Exchange System – SIX trading platform
GUI	Graphical User Interface
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transport Protocol
HTTPS	HTTP over SSL, encrypted and authenticated transport protocol
IE	Internet Explorer – Microsoft Web Browser
J2EE	Java 2 Platform Enterprise Edition
Java	Programming language and run-time environment from SUN
JDK	Java Development Kit
Linux	Unix-like operating system, open source
Log4j	Standard logging tool used in Java
OpenVMS	HP Operating system, existing platform for ERM
OSI	Open System Interconnection reference model http://en.wikipedia.org/wiki/OSI_model
RPC	Remote Procedure Call
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer – secure communication protocol with encryption and authentication
SIX Exchange	Member of SIX Group, Exchange platform provider
TCP/IP	Transmission Control Protocol / Internet Protocol
SIX Telekurs	Member of SIX Group, Financial information provider, and operational staff for ERM.

SC	Service Connector
USP	Universal Service Processor – existing middleware used by Eurex Repo
Web Service	software designed to support interoperable machine-to-machine interaction over a network
Web-GUI	Graphical User Interface running in Web-Browser built with Web components. Also called Thin-Client.
Windows	Microsoft operating system family
XML	Extensible Mark-up Language
XSD	XML Schema Definition
XSLT	Extensible Style Sheet Language Transformation

Table 1 Abbreviations & Definitions

1.4 External References

References	Item / Reference to other Document
[1]	USP Documentation http://www.stabilit.ch/index.php?option=com_content&task=view&id=27&Itemid=60
[2]	

Table 2 External references

1.5 Typographical Conventions

Convention	Meaning
text in italics	*USP feature or functionality or USP related comments*
`text in Courier font`	code example
[phrase]	In syntax diagrams, indicates that the enclosed values are optional
{ phrase1 | phrase2 }	In syntax diagrams, indicates that multiple possibilities exist.
…	In syntax diagrams, indicates a repetition of the previous expression

Table 3 Typographical conventions

In formulation of requirements words "must" and "should" have the following meaning:

Formulation	Meaning
must, must not	Strong, mandatory requirement.
should, may, need not	Weak, optional requirement. (Nice to have)

Table 4 Requirement Formulations

The terminology used in this document may be somewhat different to other sources. The chapter Glossary includes a list of often used terms with the explanation of their meaning in this document.

1.6 Outstanding Issues

Following issues are outstanding at the time of the document release:

1. Message header is encoded in ISO-8859-1 (Latin 1) or UTF-8

2 Project Definition

2.1 Existing Situation

The new EUREX IT platform needs a middleware that allows exchange of messages between its components and applications. This middleware must also allow seamless replacement of the existing USP with a new forward looking solution. Old Eurex Repo services running on OpenVMS must be able to connect via SC to the trading GUI or to other components. However SC should not be treated as a plain USP substitution. It should open new opportunities for communication of the REPO platform with new internal or external services.

Researching the market and products we found no adequate software available. The SIX Exchange is looking for USP replacement by a standard product since 5 years without any visible progress. Our sound knowledge of USP and of the EUREX computing environment leads us to the idea of developing a new solution.

2.2 Goals

The following are the overall project goals (in priority order):

1. Create simple messaging middleware for all new components within the Eurex platform
2. Replace existing USP and keep the capability of access to existing Repo services.
3. Design a simple and open message transport protocol that can be adopted by the companies that want build custom solutions based on it.

The principle is: **“as simple as possible, serving only the real needs”.**

Other important goals are:

- Operating system independence (unix, linux, windows, OpenVMS Itanium)
- Use of Open Source components (all java)
- Universal API for message-based communication
- Use of standard underlying protocols (http, ftp, smtp, etc.)
- Publishing of SC source code in the Open Source Software community.
- Publically available documentation of the SC protocol
- API for applications written in Java (server and client) and C (server only)
- Availability equal or better then USP (> 99.90%)
- Performance better the USP (>1’000 msg./sec.)
- Scalability better then USP (>1’000 concurrent clients)
- Manageability better then USP (Web-GUI for administration)

2.3 Non-Goals

The SC will not have any persistence and thus will not provide any transactional concepts or reliable messaging.

The SC will not implement any security feature. The environment where SC is used must provide suitable security features like authentication, authorization, encryption, tunneling etc.

The SC will not provide any load balancing features. Established communication session will not be redirected to another server node during its life time.

The SC will not implement any failovers features. Aborted communication must be re-established by the communicating partners. The client application must find out a service which is alive.

SC provides message transport and thus implements a message transport protocol. The transported message payload is not known to SC and will not be inspected or transformed by SC. The communicating parties must agree on the format and content of the message payload!

For the reason above, SC is not intended for direct communication to external systems like SIS, Telekurs VDF, SMF, Bloomberg or others. These systems use their own established protocols and must be connected with other middleware or can be connected to SC via a protocol-specific SC gateway that may be developed when necessary. It is the intention to publish the SC message transport protocol and allow third-parties to connect directly to SC.

2.4 Scope

The scope of the project is to design and develop the SC, including all interfaces to the existing USP applications.

Only http transport will be implemented in the first release for the underlying transport.

Only Java API will be implemented in the scope of this project. The SC client and server API for C will be developed in a separate joint project together with the customer (SIX Exchange) and is not scope of this project.

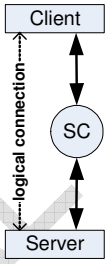
The migration from USP to SC is not scope of this development project. It will be planed and subsequently realized as a separate project.

2.5 Relationships & Dependencies

The USP migration to SC cannot begin before this project will finish and the acceptance test is passed. However it is possible to start developing the necessary adoptions of the connecting applications as soon as the SC interface has been published.

3 Requirements

The SC must support message exchange between requesting application (client) and another application providing a service (server). The client and the server are the logical communication end-points. The SC is always in between of these points and establishes the logical connection between the communicating partners. It never acts as a direct executor of a service. In order to enable the communication, the SC must run all the time.



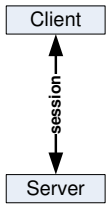
The client must be able to communicate to multiple services at the same time.

Server application can provide one or multiple service. Serving multiple services by one server application is possible only for multi-connection servers. Multiple server applications must coexist on the same server node, each providing different service. All services are independent on each other.

Server application may request another service and so play the client role. Such cascading at application level must be possible. Cascading of services must also be possible through the SC. The SC provides API and messaging for the following service types:

3.1 Session Services

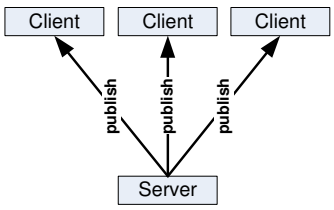
Request/Response (client initiated communication) See use case 4.1.1. For session services the client and the server exchange messages in context of a logical session through the SC.



Former USP-RPC - remote procedure call

3.2 Publishing Services

Subscribe/Publish (server initiated communication) See use case 4.1.2 and 4.1.3
Publishing services allows the server to send single message to many clients through the SC. See use case 0.



Former USP-BCT – broadcast

3.3 File Services

This SC service provides API for these file operations:

- Download file from the web server to the client. See use case 4.1.4
- Upload file from the client to the web server. See use case 4.1.5
- List files in a file repository on the web server. See use case 4.1.6

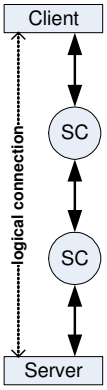
USP does not support files operations

3.4 Proxy Services

There may be multiple SCs on the path between the client and the server. Such SC cascading will be used for performance and/or for security reasons. Cascading must be fully transparent for the application.

Cascades SC services are described in use case, 4.2.1, 4.2.2, 4.2.3 and 4.2.4.
They provide:

1. Cascading of session services, publishing services and file services
2. Bundling of the network traffic for session services
3. Message caching for session services
4. Fan-out of the published messages for publishing services
5. HTTP proxy service



USP supports a slightly reduced set of proxy functions. It does not bundle traffic for session services and provides no caching.

USP-RPC implements a web server with http 1.0 protocol. Due to memory leaks in this component SWX uses a regular Apache web server instead.

4 Specifications

The SC implements peer-to-peer messaging above OSI layer-7 (application) network model between client and server applications. The SC is always in between the communicating partners, controlling the entire message flow.

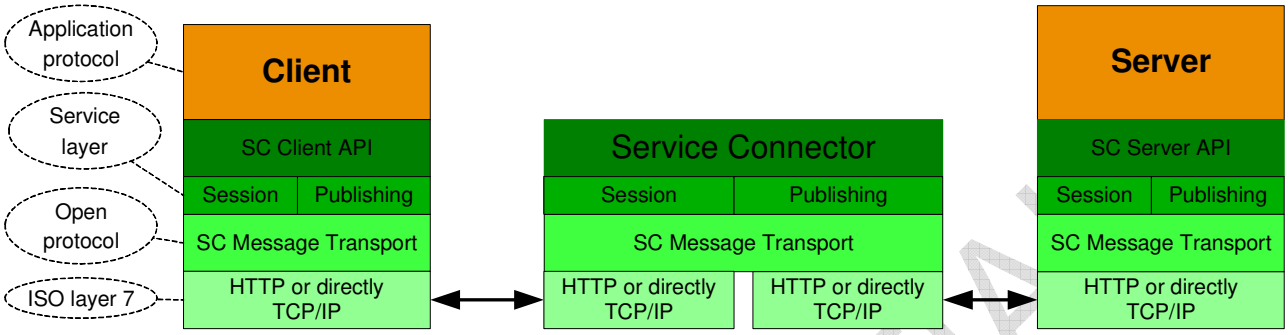


Figure 1 Communication Layers

The SC acts like a broker, passing messages between the client and the server. The communicating parties must agree on the application protocol i.e. format and content of the message payload.

4.1 Use cases

The SC implements the use cases described here below.

4.1.1 Synchronous Request/Response

The client sends a request to a service that invokes an application code. Upon completion the service sends back a response message. The client waits for the arrival of the response message. The request and response message length is not limited in size.

The communication occurs in a scope of a logical session. SC will choose a free server and pass this and subsequent requests from this client to the same server. Session information is always passed as a part of the message header. The client may have only one outstanding request per session.

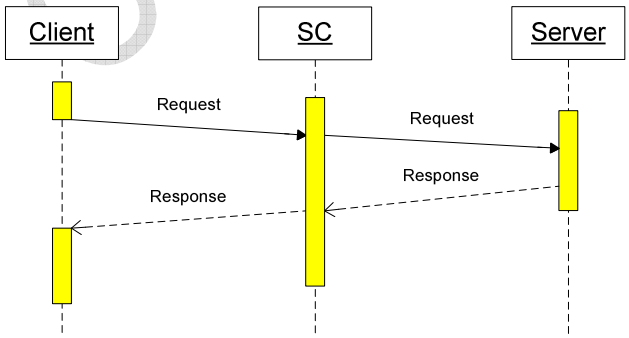


Figure 2 Synchronous Request/Response

Multiple clients may request the same service at the same time. The service execution is in parallel, each one in a separate thread or process. The server decides how many sessions it can serve.

This communication style is the most often used for getting data from the server or sending a message that triggers a transaction on the server.

USP maintains a session context. It starts and assigns a separate server process for each connected client and maintains a permanent TCP/IP connection between client, the USP and the allocated server until the client disconnects. This is very resource consuming and massively limits the scalability. Some session checks are in the server application (ICS, TXS, TXR) itself.

4.1.2 Asynchronous Request/Response

This is functionally equal to the synchronous case with the exception that the client does not wait for the arrival of the response message. The client must declare a notification method that is invoked when the response message arrives. The client may have only one outstanding request per session. When client issues a request before the previous one was completed, the send method blocks until the previous request is satisfied.

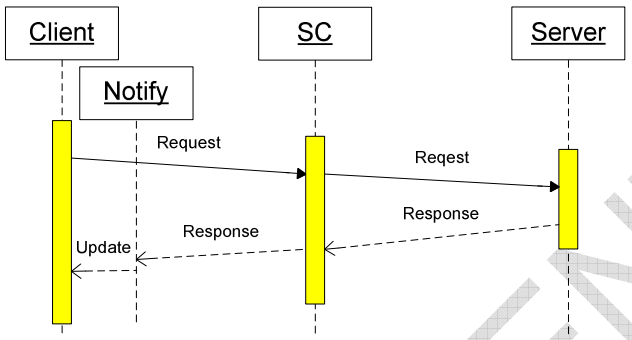


Figure 3 Asynchronous Request/Response

This communication style will be used to load data while other activities are in progress, e.g. to get large amount of static data at startup. It can be also used as fire-and-forget when the response is not meaningful.

USP does not support asynchronous request/response.

4.1.3 Subscribe/Publish

The client sends a subscription mask to the service, and so declares its interest on certain type of a message. The application service providing the message contents must designate the message with a type. When the message type matches the client subscription mask, the message will be sent to the client. Multiple clients may subscribe for the same service at the same time. In such case multiple clients can get the same copy of the message. Message that does not match any client subscription is discarded.

The client must declare a notification method that is invoked when the message arrives. The client may have only one outstanding subscription per service. The message delivery must occur in guaranteed sequence. Messages from the same service will arrive in the sequence in which they have been sent.

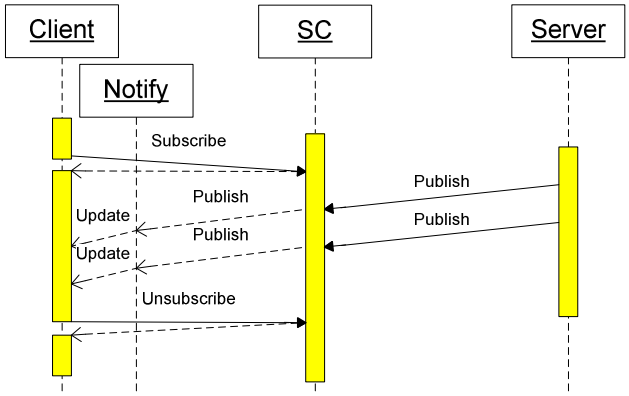


Figure 4 Asynchronous Subscribe / Publish

The client may change the subscription mask or unsubscribe. Initial subscription, subscription change or unsubscribe operation is always synchronous, even through a SC proxy.

Such communication style is used to get asynchronously events notifications or messages that are initiated on the server without an initial client action. It can be also used to distribute the same information to multiple clients.

USP implements a broadcasting service identical to the functionality described above. It queues messages that are later distributed to the clients. This can cause exhausting of memory when the client is not able to receive the messages and the connection is not aborted (e.g. blocking firewall in between)

4.1.4 Download File

The client sends a request to download a file via SC from the web server. The downloaded file is stored locally on the node where the request was issued. Only download via HTTP will be supported. WebDAV protocol will not be supported. The communication style is synchronous. Standard Apache web server can be used.

This service will be used to download the actual SC-proxy configuration from a central server. This service can be also used by the client application to download other files.

USP does not support file operations

4.1.5 Upload File

The client sends a request to upload a file via SC to the web server. The uploaded file must exist on the node where the request was issued. Only upload via HTTP will be supported. WebDAV protocol will not be supported. The communication style is synchronous. Standard Apache web server can be used.

This service will be used to upload log files from SC-proxy to a central server. This service can be also used by the client application to upload other files.

USP does not support file operations

4.1.6 List files

This service is indirectly supported by the standard web server (e.g. Apache) when directory browsing is allowed and enabled. The client sends an URL and gets back a HTML formatted output containing the file list. The client must parse this response in order to evaluate the exact file names. This communication style is synchronous. Standard Apache web server functionality is utilized.

This service will be used to get list of configuration files on the server that can be downloaded. This service can be also used by the client application to see which files can be downloaded.

USP does not support file operations

4.2 Proxy Services

For the client and the server the SC always acts like a regular component, but for dedicated services it may pass all messages to another SC with the same service name and type. This "cascading" is possible for all service types.

4.2.1 Session Services

For proxy session services the SC bundles requests from multiple clients and passes them to another SC like a single client. Received response messages are passed back to the appropriate clients. The purpose of bundling is to use only few communication connections and so save resources.

Each time a client is started usually a high volume of static data must be loaded from the server. Most of this data is static i.e. valid for a long period of time and is accessible for all clients. In order to shorten the start-up time of the clients SC should implement a message caching mechanism for dedicated server content. The purpose of the cache is to store shared data as close to the clients as possible.

The client request for a cached content will differ from regular request. The corresponding server response will be stored in the SC and can be used by other clients. The cache content is refreshed when its time-to-live expires and some client sends a request for it. The SC cache is volatile and is discarded when the SC is restarted.

USP-Proxy does not provide bundling of Request/Response traffic into a single connection and thus overloads the server with thousands of parallel connections. USP-Proxy does not implement message caching. Client start-up takes up to 10 minutes.

4.2.2 Publishing Services

For proxy publishing services the SC combines client subscriptions to a single subscription mask and provides fan-out (distribution) of received response messages received to the subscribed clients according to their subscription mask. In this ways the SC uses only few downstream connections.

USP-Proxy implements identical fan-out features.

4.2.3 File Services

For proxy file services the SC passes the data to another SC like a single client. The final SC in the path is then communicating with a regular web server. No file caching will be implemented in the SC for the file services.

USP-Proxy and USP do not support files services

4.2.4 HTTP proxy

SC node is often located in DMZ at the customer site and connected via VPN with the server. Therefore it must also provide simple HTTP proxy service, because it represents the only path to the server node where a regular web server (apache) is running.
No caching will be implemented in the SC for the http proxy service. The requested url must be resolved (dns) by the underlying network infrastructure. SC does not support any name resolution.

USP-Proxy implements http 1.0 redirection without caching.

4.3 Servers

SC will support services implemented in servers. Servers are always pre-started and register themselves on SC. Two different server types are supported:

- Single-Session servers.
  One server process is dedicated for a single session. This is the case in actual ERM architecture.
- Multi-Session servers.
  One server may serve multiple sessions and/or multiple services. E.g. Apache Tomcat can be used to implement such services.

USP supports single session servers only

4.4 Service Naming

The network represents the namespace domain. The service names within this namespace must be unique. Therefore services residing on different server nodes within the same network must have different names.

USP behaves the same way.

4.5 Network

Client application, server application and the SC may reside on the same node or on separate nodes connected via TCP/IP network. No assumption about the physical network topology must be done. Multiple firewalls can be located on the path between the communicating applications.

UDP must not be used, because it will not pass firewalls and routers. FTP should not be used because it will not pass customer firewalls and may cause potential problems with customer security policy.

SC is not supported on network with nodes having mixed architectures (big and little endian).
SC is supported only on nodes with ASCII character set (no support for EBCDIC).

USP has the same limitations

The system must be able to handle network size defined in the following table

Item	Number	Comment
Clients	≥10'000	Currently 1'100 users are registered
Proxies	≥1000	Currently 250 USP-Proxies are in use
Services	≥100	Currently 2 nodes with 13 services each are in use

Table 5 Network Size

For technical reasons USP supports <1000 concurrent client.

4.6 Connection Topology

The SC supports following connection topology:

- Client ⇔ SC ⇔ Server = Direct connection
- Client ⇔ SC ⇔ SC ⇔Server = Connection via cascaded SC.
  Multiple SCs may be placed on the path between the client and server.

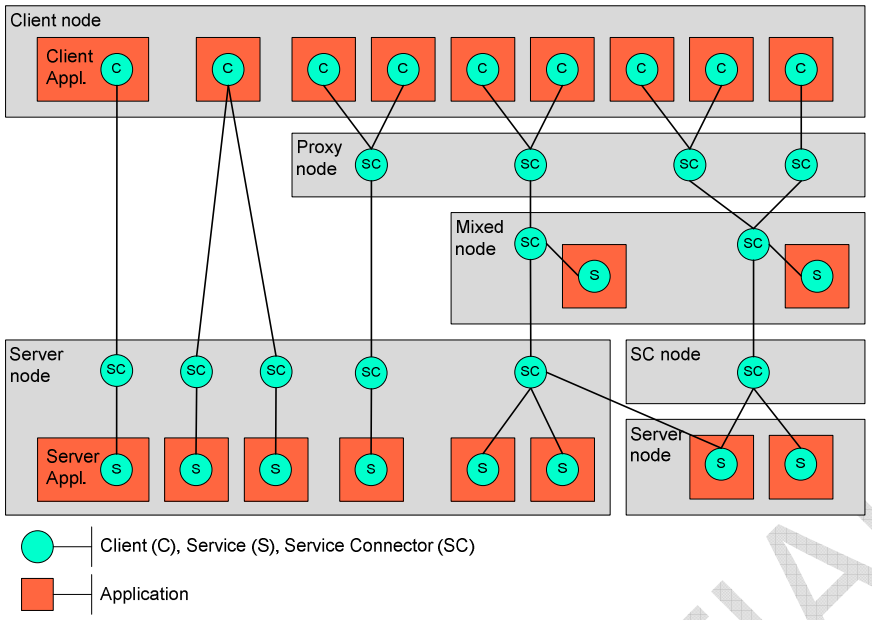


Figure 5 Connection Topology

Different connection topology types from left to right:

1. Client connected to one service
2. Client connected simultaneously to SCs and two services
3. Two clients connected to one service via proxy service and cascaded SC
4. Two clients connected to three services via proxy service on different server nodes
5. Complex configuration with three clients connected to three services on different server nodes via cascaded SCs and SC offloaded to its own node. One server can be registered to multiple services and different SCs. However this is possible for multisession servers only.

Limitation: The same service can be accessed by one SC only. When the same service should be used on different nodes, it must have a different name (e.g. node suffix).

4.7 Underlying Message Transport

Two different transport types can be individually configured between the Client ⇔ SC, SC ⇔ SC or SC ⇔ Server.

1. Over HTTP
   Such connection may pass screening firewalls and is appropriate for communication within the customer organization e.g. Client ⇔ SC or SC ⇔ SC.
2. Direct TCP/IP
   Such connection would not pass firewalls without explicit security rules. It is useful for connection within the same node e.g. SC ⇔ Server.

In the future it should be possible to implement other message transport protocols later without changing the client or server API.

USP uses a proprietary binary communication protocol over TCP/IP and over DECnet.

4.8 Message Format

The message consists of a variable size header and variable size body = payload.

Message header content belongs to SC. Its structure is published. Java API will be provided to get important attributes. Messages header is encoded in ISO-8859-1 (Latin 1) character set.

Message body content belongs not to SC and is transported as a block of bytes (8bit). For publishing services the maximum message body length is 64kB. For session services the maximum message body length is not limited. If it is > 64kB then it will be transmitted in chunks. (The 64kB limitation is caused by I/O buffer size on OpenVMS)

It is the task of the communication partners to agree on its structure and format as well as to perform appropriate marshalling or de-marshalling of data types.

SC supports message body compression (ZIP) and de-compression during the message transmission. This can be enabled or disabled in the configuration, but not for a individual message.

USP does implement marshalling / de-marshalling of some standard data types (string, integer and float) but this is not used by SIX. Message body compression is implemented on application level. USP message limit is 64k.

4.9 Message Delivery

Messages to session services are delivered in the transmission order specified by the client. Because only one request may be outstanding for a particular session, the server responses are delivered back in the same order. The request or response message is delivered at once or not at all. In such case the communicating parties will detect a transmission error.

Messages to publishing services are delivered to clients in the order the SC receives them from the publishing server. When multiple servers publish messages to the same service, the delivery order to the clients is not predictable. The published message is delivered to the client at once or not at all. In such case the client will detect a transmission error.

4.10 Keep-alive Messages

When no real data is exchanged, the communicating parties and the SC exchanges periodically keep-alive messages that allow the detection of the connection state.

The keep-alive message should also be used to exchange time information between communicating parties and SC. This does slightly simplify troubleshooting and operation in different time zones. It also allows the client do measure the round trip performance.

USP does implement keep-alive for request/response in V3 protocol. This is not used by SIX Group. Instead the V2 protocol is used and keep-alive is implemented at application level. For subscribe/publish complex and cumbersome keep-alive messages are implemented, but this does not work reliably.

4.11 Automatic Reconnection

For performance reasons connections over HTTP will not be established for each individual request, but kept over longer time. Event thought the HTTP protocol is stateless and connection could be recovered at this level, the parties are bound in a logical session and thus maintain a state. Long breakdown of the connection must cause session cleanup. For this reason automatic reconnection is not possible.

USP does not have an automatic reconnection or connection recovery and aborts both connections to the parties.

4.12 Load balancing

The SC does not provide any load balancing features. Established communication session will not be redirected to another server node during its life time.

USP does not implement load balancing. This is built into the DDC application.

4.13 Failover

The SC does not provide any failover features. Aborted communication must be re-established by the communicating partners. The client application must find out a service which is alive.

USP does not provide any failover features.

4.14 Security

The SC does not implement any security feature. The environment where SC is used must provide all required authentication, authorization, encryption, tunneling etc. features. Message transport over https will not be supported.

USP provides SSL communication in cooperation with Apache CSWS, however no customer is using this feature.

The IP address of the client and the IP of the incoming TCP/IP traffic must be stored in the message header and can be obtained via API within the server. This can be used to authorize the client when a VPN tunnel is used.

USP follows the same philosophy and has the same limitation.

4.15 Intrusion and Virus Protection

The entire network where SC is used is assumed to be safe and secure. No virus protection is embedded in SC. The customer may use screen firewall to protect the SC components. It is recommended to use SC within a DMZ.

SC is not designed to withstand network attacks like DOS or SYNC flood, or any other.

4.16 Deployment

The SC client and server APIs for java will be delivered as one jar-file.
The SC client and server API for C is not scope of this project.

USP provides client and server API for C and LEVEL4 and a client API for Java. C API is not used. C applications are wrapped with LEVEL4 code.

The SC is delivered as jar-file that can be started from the command level as a java application (runnable jar-file). Regular services and proxy services can be configured on the same instance. Multiple instances of a SC must be able to run on a single node. Each instance must have its own configuration.

On Windows platform SC can be deployed as service.

USP is deployed as a OpenVMS kit, USP/Proxy is deployed as ZIP file. USP Java Client is available as ZIP file (source code).

4.17 Configuration

The SC components embedded in the application are configured through the corresponding API. The configuration of SC is file based. The format of the configuration file is ASCII. (XML is not friendly for editing!)

The configuration contains static (S) and dynamic (D) parameters. Change of static parameters cannot be changed at run time and requires SC restart and thus los of all connections. Dynamic parameters can be changed at run time.

The SC configuration defines:

- (S) Log file location
- (D) Log level
- (S) Nr of days to keep log files
- (S) Administration port (for admin GUI)
- (S) Administration username (plain)
- (S) Administration password (plain)
- For each implemented transport parameters like
    - (S) Transport protocol (HTTP or plain TCP/IP)
    - (S) Port number
    - (S) Other transport specific attributes

The SC configuration defines on service level

- (S) Service name
- (S) Service type
    - (S) downstream SC node or IP (for proxy service)
    - (S) downstream SC port (for proxy service)
    - (S) downstream transport protocol (HTTP or plain TCP/IP)
- (D) Log level
- (S) Log filename prefix
- (D) Flags that allows / disallows client connections
- (D) Maximal number of active clients (for Request/Response services)
- (S) Size of the subscription mask in bytes (for Subscribe/Publish services)

USP has a proprietary binary configuration file format. Some parameters are dynamic and can be changed at run time without USP restart. However this causes a connection loss to affected clients and services.

4.18 Administration

No administration features are available for the client or service. These components are embedded in the application and accessible via SC API.

The SC and SC-Proxy administration is reduced to proper configuration.

4.19 Operation

The SC must provide reasonable tools for local operations. These are:

- Start SC
- Stop SC
- Enable or disable connection to a particular service
- Change dynamic configuration parameters
- Get information about the actual service state in order to pre-start more servers.
- Download new SC configuration from a server

Remote operations are not supported.

The client and server applications are started, stopped and managed by operational facilities that are not scope of the SC. The client may be started and stopped at any time. The session server must be pre-started and must register itself on SC as a service provider before the first client will need its service.

4.20 Monitoring and Troubleshooting

The SC must provide reasonable tools for local monitoring and troubleshooting. A monitoring Web-GUI should be implemented and should provide following features:

- Show state of all services or a particular service
- Show statistic of all services or one service
- Show the log file
- Upload selected log files to a server

The Web-GUI must not make any assumptions about the plug-ins used by the browser. IE V6.0 or later and Firefox 3.0 or later must be supported.

All components (Client API, Server API, SC) must provide:

- Multilevel logging facility (log4j) with the following levels:
  - Connection (connects, disconnects, abort, loss of connection, re-connect, etc.)
  - Message header

SC and SC-Proxy must additionally provide:

- Statistical information
  - Actual version number
  - Configuration file loaded
  - Start-up timestamp
- Statistical information per service
  - Total nr. of connections
  - Total nr. of re-connects
  - Total nr. of messages sent
  - Total nr. of messages received
  - Average message size sent
  - Average message size received
  - Maximal message size sent
  - Maximal message size received
  - Actual subscription mask (Subscribing client only)
  - Actual number of connected clients (Publishing server only)
  - Actual number of executing clients (Responding server only)

USP has a utility to get limited run-time information.

4.21 Operating environment

The SC client and server components should run on any operating system supporting Java 6. Typically the client components will run on Windows or Unix platforms. The SC and server components can run on OpenVMS Itanium at the first stage and later on Linux.

SC will not run on OpenVMS - Alpha because this platform does not support Java 6 (but only JDK 1.5)

4.22 Visibility

The Service Connector will be published to SourceForge as Open Source Software. Also the source code will be publically available.
Client and proxy components will be used at Eurex and can be also distributed to selected EUREX customers.

4.23 Licensing

The SC will be available under Apache 2.0 software license.
http://www.apache.org/licenses/LICENSE-2.0.html

4.24 Availability

This software is the connection between the banks and the exchange and is classified as business critical. The required yearly availability is 99.9 % on regular business days (Monday to Friday), during extended business hours 6:00 – 22:00.

4.25 Performance

SC must be capable to transport >1000 msg./sec. (request/response, client and server on the same node, message length 128 bytes)

USP/RPC reference benchmark can handle 600 msg./sec, each 128 byte long on AlphaServer 800 under OpenVMS 8.1

4.26 Language

English (U.S.) language must be generally used for all project documentation and software components including user interface, configuration and administration. Other languages will not be supported. Documents in German language are not allowed.

4.27 Flexibility Constraints

It must be possible to add new transport methods. This must not have impact on the API.

4.28 Documentation

SC package must be delivered together with the following documentation:

- Programming Guide
- JavaDOC for Client and Server API
- Operation Guide containing the chapters:
    - Concepts
    - Configuration
    - Operation
    - Troubleshooting

5 Glossary

Service

The term service is used as synonym for a piece of application code that implements a certain function.

Client

The term client designates the application requesting a certain service.

Client node

Client node is physical network node (machine) on which the client application resides.

Server

The term server designates the application providing a certain service.

Server node

Server node is physical network node (machine) on which the server application resides.

Message payload

Message payload is part of the transported message containing the application data. SC does not inspect, transform or interpret the payload. It is the responsibility of the communicating partners to define the format, syntax and semantic of the payload.

SCMP => SC Message Protocol

Is a publically presented protocol used for communication between client, SC and the server. In the OSI layer model, message transport protocol is immediately above the application protocol layer 7.

Message transport format

Format of messages transported messages between client, SC and the server. It consists of a header and a payload.

RR => Request / Response

This is basic communication style. The client requests an execution of a (remote) service and gets back the results in form of a response. The execution may be blocking - clients waits for the response, or non-blocking (asynchronous) – the clients does not wait for the response. Sometimes it is also called Remote Procedure Call = RPC.

SP => Subscribe / Publish

This is another popular communication style. The client tells the server what he is interested in and gets the data from the server later when a event arise. The execution is always non-blocking (asynchronous) – the client does not wait for the data receipt. This is because the event occurs on the server.

Appendix

Appendix text

Index