

|  |
| --- |
|  |
| Mobile Authentication Corporation |
| Secure Trading Registration Service API, Version 1.1 |

|  |
| --- |
| Terry Davis  6-27-2014 |

# Introduction

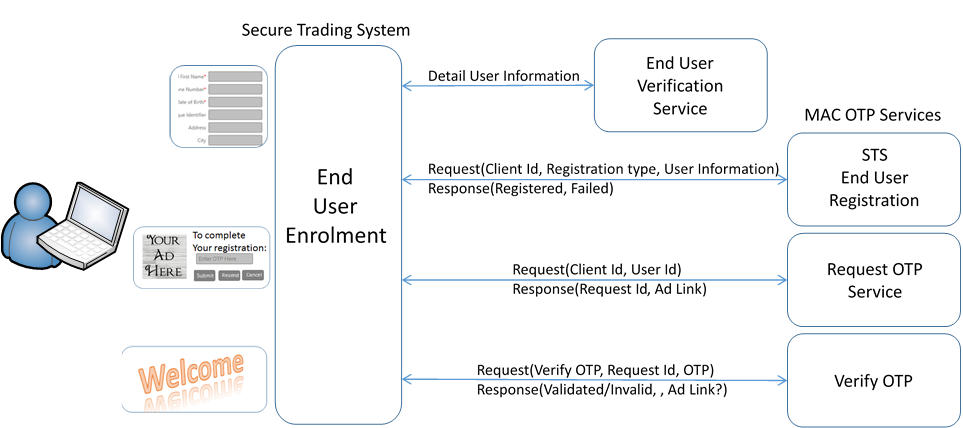
This document defines the API for the Web Service that *Mobile Authentication Corporation* (MAC) has provided to *Secure Trading System* (STS) for use in STS’s *End User* Enrollment process to register *End Users* with the MAC OTP *System* (System).

The System is comprised of several Web Services (Services) that provide the functionality needed to *register* the *End Users*, Request a *One-Time Password* (OTP) be sent to the *End User* and to *verify* the OTP entered by the *End User*.

Overview

Contained in this document are brief descriptions of the HTTP/HTTPS methods for sending requests to the Services, the responses, the message formats, and the client requirements. The document also contains JavaScript/JQuery examples of the functions which create and issue the calls, as well as, process the responses.

## Registration diagram



Clients

In the context of the MAC OTP System, Clients are the “Operators” those entices the system is being run for, Casino operators, Merchants, Banks, etc. The MAC system requires every client to be registered with the system. When registered, the client will be issued a ***Client Id***. Every request issued to one of the Services must contain a valid Client Id. Optionally, the system supports the concept of a **Group.**  A group is a collection of one or more clients.

**Note**: Examples in this document do not have Group Ids.

## End Users

In the context of the MAC OTP System and this document “*End Users*” are the customers of the Clients. The *End Users* are the people that receive the OTP messages on their message enabled devices. The System expects *End Users* to be verified by the client and/or be registered with the System. In the “Client Controlled” API calls it is the responsibly of the client to insure that the end user’s phone number and email address are valid. The System only checks the client id and the format of the phone number and email address. In the “Registered” API calls the end user must be registered before the OTP requests are processed by the System. The phone number and the email address are maintain in the System database. The Service API requires that the caller provide a unique UserId when issuing requests to the System.

# Secure Trading Registration Service

This service was developed to service requests from the STS Enrollment process. This service assumes that the End User and the End User information have been verified and format checked before being passed to the service. The base URL (where the Services are running) combined with the Service URL make up the HTTP address for the requests.

STS Registration: /User/STSEndUserRegistration.asmx/WsSTSEndUserRegistration

## Service API Requests

This service support the HTTP/HTTPS Post method where the data contains the request details. Depending on the implementation, the data is either converted to hexadecimal strings or encrypted (recommended when using HTTP) before making the request.

## Request Format Details

The parameters for a request are assembled in an ASCII string as a key value pair with each key/value separated by the pipe character “|” and the key separated from the value by the colon character “:”. If the value “could” contains a colon character, the value must be converted to a hexadecimal string before it is added to the request parameters. (See the coding examples section for details).

* Example of JavaScript function call

function STSRegisterEndUser(

pClientId, // Client Id (required)

pFirstName, // Legal first name of end user

pLastName, // Legal last name of end user

pPhoneNumber, // End user’s phone number

pEmailAddress, // End user’s email address

pUserId, // Unique User Id (Secure Trading’s User Id)

pCallbackFunction)

* Example before hexadecimal encoding:

**Note**: Key value pairs with keys in red and values in blue (key value separator is in black).

Request:EndUserRegister|CID:53ac9ff0748469131c17872d|FirstName:John|LastName:doe|PhoneNumber:9995551212|EmailAddress:jd@gmail.com|RegType:ClientRegister|UserId:ED5D0C76F8E7B6D37621CE63447D984B|API:STS

Where:

1. The request : Request: EndUserRegister
2. Client Id : [CID:](CID:5351674c74846919ec735074) 53ac9ff0748469131c17872d
3. End user’s first name: FirstName:John
4. End User’s last name: LastName:Doe
5. End user’s mobile phone number: PhoneNumber:9995551212
6. End user’s email address (required): EmailAddress:jd@gmail.com
7. Registration Type: RegType:ClientRegister
   1. ClientRegister: Only the client that registered the end user can use the end user.
   2. GroupRegister: Any client that belongs to the “group” can use this end user.
   3. OpenRegister: Any registered client can request OTPs can use this user.

Note: The client must use the UserId that the user was registered with.

1. UserId (optional) is a unique id generated by the caller, in this case the STS enrollment application.
   1. If the UserId is not supplied with the registration request the end user’s email address will be used.
2. End user’s machine IP address (optional): EndUserIPAddress:192.168.168.1
3. Who is making the request (optional, used for resolving errors): API:STS

* Example after hexadecimal encoding (complete data packet):

Data=

* Break down of components:

Http post header: Data=

Hexadecimal encoded indicator: 99

Length of client id: 24

Client id (as issued by MAC): 53ac9ff0748469131c17872d

Request data (Hexadecimal encoded): 

## Response Formats Details

All the OTP Services responses are formatted in XML. Responses contain a Reply node if successful and an Error node if unsuccessful.

* Example of response to successful request:

<?xml version="1.0" encoding="utf-8" ?>

<macResponse>

<calledMethod>WsSTSEndUserRegistration()</calledMethod>

<Reply>Registered</Reply>

<Details>RegisteredSTSEndUserRegistration:ClientRegister, New State=Registered<Details>

</macResponse>

* Example of response to unsuccessful request:

<?xml version="1.0" encoding="utf-8" ?>

<macResponse>

<Error>End User Exists</Error>

</macResponse>

## Optional End User Information

The MAC OTP system has the ability to secure store additional End User information if needed. In the current implementation none of the OTP applications use this data.

Name:

Prefix

First

Last

Middle

Suffix

Mobile Phone Number

Email Address

Date Of Birth

Last 4 digits of Social Security Number

Primary Address:

Street

Street2

Unit

City

State Code

Zip Code

Country

Driver License

State of issue