

MAC OTP System

# Overview

DynaPass and MAC held technical review meetings at DynaPass offices to discuss the architecture and review the state of the system and what parts required additional development to make the product “financial grade” and able to meet the requirements of a product to be marketed to the financial services industry.

# Technical Meeting

In the technical meeting at the DynaPass offices the participants realized the DynaPass system, although feature rich would have to be re-architected to address the requirement of the financial services industry. The participants outlined a basic architecture “on the white board” and discussed several of the key points such as the separation of functionally, operation and administrative control and access to data.

# MAC Business Meetings

MAC held business meetings on October 21st and 22nd to discuss the OTP system and how it would work in the different environments of the current customer base. Subjects discussed as it relates to the system where ***Registration, Configurations, Authentication and Transaction Verification, Transaction flow*** between the different participants, and Service levels.

Contents

[Overview 1](#_Toc372283557)

[Technical Meeting 1](#_Toc372283558)

[MAC Business Meetings 1](#_Toc372283559)

[Architecture 3](#_Toc372283560)

[Architectural Concepts 3](#_Toc372283561)

[Registration 4](#_Toc372283562)

[Components 4](#_Toc372283563)

[MAC Clients 4](#_Toc372283564)

[OTP Server, OTP and Ad Databases 4](#_Toc372283565)

[Registration Server 4](#_Toc372283566)

[Archive Server 4](#_Toc372283567)

[CRM Server 4](#_Toc372283568)

[OTP Text Message Construction 4](#_Toc372283569)

[Requirements 6](#_Toc372283570)

[OTP Service 6](#_Toc372283571)

[OTP Server API 8](#_Toc372283572)

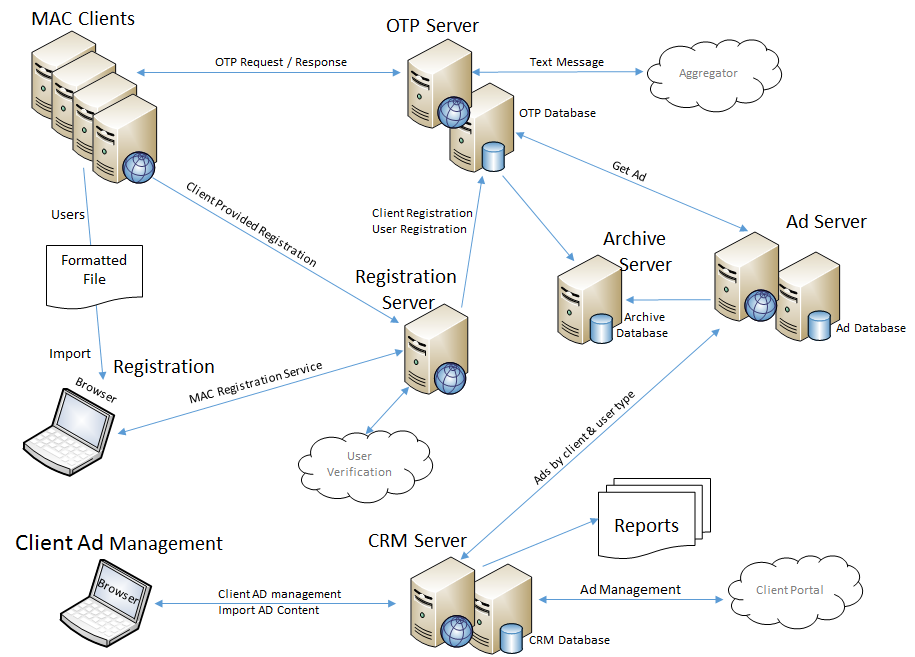
[Registration Service 9](#_Toc372283573)

[Archive Server 9](#_Toc372283574)

[CRM Service 10](#_Toc372283575)

[Definition of Terms 11](#_Toc372283576)

# Architecture



## Architectural Concepts

Note: In the above architectural diagram it is important to understand the use of the term “Server” and “server” are equivalent terms.

Provide the MAC system as a Software as a Service or dedicated service implementation.

The separation of MAC system features/services based on the different business entities that are found in most finical organizations. This allows best fit deployment based on the client.

Data at Rest security generally refers to data stored in persistent storage. Any data considered as sensitive data that is stored by the system shall be encrypted using an industry standard encryption scheme.

Clients (tenants of the system) is an organization has contracted with MAC to use or run all or specific services of the MAC system.

Support multiple message service providers (aggregators or gateways) for SMS, Voice & email.

Performance is a primary concern of the architecture where the most used components of the system are stream lined to prevent excessive network and/or disk activity.

### Registration

The registration must be implemented as to provide multiple levels of service ranging from **Full-Service Registration** to **Client Managed Registration** and **Client Only Registration**. Registration must support the concept of **Open Registration**.

**MAC Full-Service Registration** is a Web Site hosted by MAC that Clients could redirect their end user to in order to register for the OTP service. MAC would provide custom enrollment pages for each client and maintain user data on MAC servers.

**Client Managed Registration** is a Web Service provided by MAC that would allow MAC approved clients to register the client’s end users. The type / amount of user information that is maintained at MAC.

**Client Only Registration** is the process where only the client is known to MAC. End user information is maintained by the client.

**Open End-user Registration** is where an end-user can be registered and use the OTP service at any registered client.

**Restricted End-user Registration** is where the client can restrict the end-user’s OTP usage.

## Components

The MAC system is architected into a set of Web services and Web Applications that provide the various system features. This allows the system to be so that the system can be deployed based on the client’s business and performance requirements.

### MAC Clients

MAC Client systems are servers running in the client data processing centers. The servers will have connections to the web and have the ability to make web service calls to the OTP and Registration Servers as needed.

### OTP Server, OTP and Ad Databases

The OTP Server runs the OTP and Secure Ad functionally providing web service calls to send and verify the OTP. The OTP functionally validates the client and based on the client’s configuration the services generates the OTP, constructs the OTP text message and send the text message. The SecureAd functionally is run as an add-in option where only the client configuration will need to change in the OTP system.

### Registration Server

The registration server provides several levels of registration services. The Server supports a Web Site and Web service calls to allow MAC or its clients to register the various participants in the OTP Service.

### Archive Server

The archive server provides the “up to date” history of OTP activity for the OTP system. The archives server will be the source for most of the online time reporting.

## Ad Server

The Ad Server is responsible for managing the Ads for each client using the OTP system and participating in the AdPass feature. The Ad Server will maintain the Ad database that is independent of the OTP database. The Ad server will return Ad text that can be imbedded in an OTP text message. Currently it is assumed that ads will be stored based on client (client id) and end-user category.

### CRM Server

The CRM server is used to maintain client activity as well as the portal for ad management.

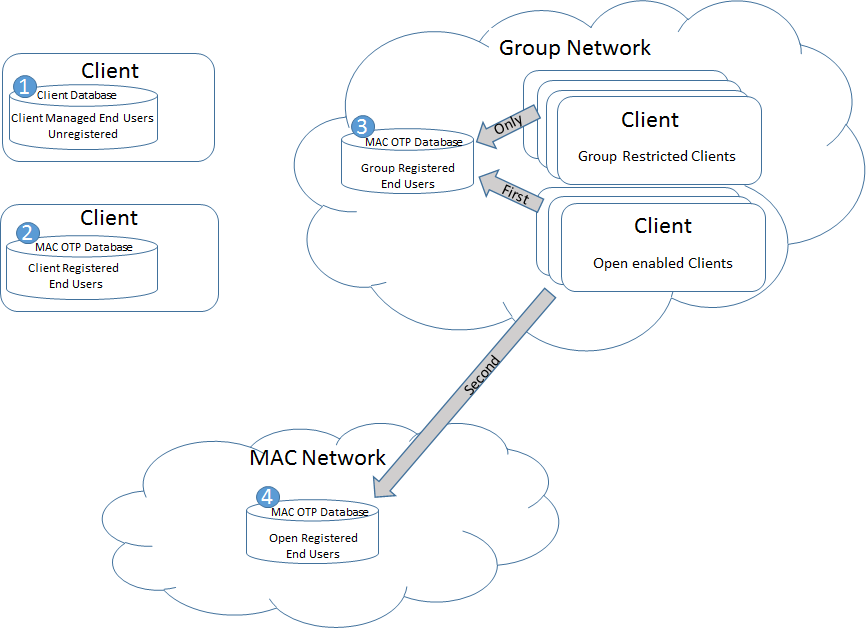
TBD

# Registration

The MAC OTP system supports four (4) methods to “target” end users being sent one time passwords at the request of a client:

1. Client Managed End User – Where the client maintains user information, name, phone number, email address, etc. The client is responsible for making sure that the end user information being sent to the OTP system is correct.
2. Client Registered End User – Where the client uses the registration service to verify and maintain the end user’s information in the OTP system. The end user is only known in the client’s OTP system.
3. Group Registered End User – Where the clients belong to a group. Their end user are registered to the group and are known to all clients in the group.
4. Open Registered End User – Where end users are registered in the MAC network and therefore known to any client that is participating in the MAC network.

## Overview



# OTP Text Message Construction

[Client Header] [OTP Label]:[OTP] [Client text (optional)] [Ad (optional)][Trailer]

* Client Header: Preset text specified when client is registered.
* OTP label: Preset text specified when the client is registered and based on the transaction type.
* OTP randomly generated text string where character set and length defined as the client is registered.
* Client text (optional): Passed in the Send OTP request. Normally used to pass transaction details.
* Ad (optional): OTP service requests ad test from the Ad Management Server.
* Trailer (optional): Preset text from client record that is appended to the end of the text message.

# Requirements

## OTP Service

The OTP service is a web service that runs in the OTP Server.

The OTP service:

1. Shall be developed as an independent web service capable of being deployed to a company service or a client service.
2. Shall be capable of operating without a user interface.
3. Shall use an SQL database to access configuration and support the OTP transaction activity.
4. Shall be developed using best practices as to allow unlimited scalability when deployed in a cloud environment.
   1. In the cloud environment OTP service shall be added dynamically based on load.
5. Shall be developed to avoid dead locks or transaction serialization when accessing the database.
6. Shall be capable of sending the OTP message via SMS, Email or Voice.
   1. Voice (a future option) shall consider user’s selectable language.
7. Shall be capable of routing text messages to one or more aggregators based on the client’s configuration.
8. Shall be capable of creating the OTP text message formatted and have content based on the client’s configuration and the Send OTP request.
   1. The text message shall be compliant with the requirements of targeted aggregator.
9. Shall support the following web service calls:
   1. Send OTP Request containing the Client Id, User Type, Transaction Code and Optional Text where:

***Note***: Does starting a session limit the number of OTPs that can be outstanding at one time. Would using a request id make more sense?

* + 1. The Client Id shall be given to the client what registered.
    2. The User Type shall be a code used by the Ad management Service.
    3. The Transaction Code shall be a single digit number used to select the OTP label.
    4. Optional Text shall be a string of characters the client wants to send as part of the OTP message.
    5. Response shall contain a Request Id and the status, where the status shall be
       1. OTP sent
       2. OTP not sent
  1. Verify OTP (No session option) containing the OTP Request id and the OTP
  2. Verify OTP (Session option) containing the Client Id and the OTP
  3. Send OTP Request details
     1. The Responses to the Send OTP request shall contain the Status and the Request id.
        1. The response status shall be OTP sent, OTP not sent system error.
           1. Shall retry a send text message request to the aggregator.
        2. The request Id shall be a unique number generated by the OTP service for each send request.
     2. Shall log all Send OTP Requests and Responses.
     3. The client shall be responsible for retrying a failed send OTP request.
     4. Shall be capable of validating the client id before sending the OTP message.
     5. Shall construct the OTP with the following parts:
        1. The “Client Header” shall be a short string of text characters that starts every OTP message sent for the client. The header is used to identify the sender to the end user.
           1. The header shall be preset value configured when the client is registered.
        2. The “OTP label” is a short string of text characters that directly precedes the OTP.
           1. The label shall be based on the client and the transaction type.
           2. Labels shall be preset values configured when the client is registered.
        3. The “OTP” a randomly generated string of characters based on the client id.
           1. The OTP generator shall generate OTP preset length.
           2. The OTP generator shall generate OTPs from a preset character configured when the client is registered.

Preset character set shall support: only numbers, only upper case characters, only lower case numbers and mixed characters.

Mixed character sets shall not include characters the can be confused between a numeric or alphabetic characters (Look-A-like), such as O, L and I.

Mixed character set shall include special characters.

Look-A-like characters shall be not be included in the character set.

Small special characters shall be not be included in the character set, such as commas, periods, single quotes, etc.

HTML special characters that may cause issues with web pages shall not be included in the character set, such as the greater than sign, etc.

* + - * 1. Optional Client Text shall be passed in the “Send OTP request”.

Shall support an option to filter out any unwanted words from the test.

* + - * 1. The Secure Ad functionally “when available” will be run as a dynamic add-in component called by the OTP message assembly function based on the client and user information.

1. Shall log all activity
   1. Log entries shall include Send OTP Requests and responses and Verify OTP Requests and responses
   2. Log entries shall contain the text message.
   3. Log entries shall contain the phone number.
   4. Log entries shall contain the aggregator id.
   5. Log entries shall contain the delivery method (SMS, Email or Voice).
2. Shall maintain usage totals
   1. Usage totals shall be available via web service call
   2. Usage totals shall be capable of being sent on a schedule via email or text message

### OTP Server API

Notes:

1. Client’s API key should not be static
2. Request block should be encrypted (what is the key)

#### SendOTP Request and Response

URL URL of Service

Request SendOTP

?p1=key Client’s API key

&p2=UserUID User Unique generated by the client using the MAC supplied applet.

&p3=IP End user’s IP

&p4=(0-9) Request Type used to select the OTP label from the client collection.

&p4=Client text Optional, Note: Transaction details

Response:

Response Code Successful OTP sent, OTP request number

Failed

Invalid client id

Invalid user id

Invalid request (format)

#### VerifyOTP Request and Response

URL URL of Service

Request Verify OTP

?p1=key Client’s API key

&p2= OTP request number

&p3=OTP OTPto verify as entered by the end-user

Response:

Response Code Valid,

Invalid

Did not match,

Timed out,

Invalid request number

## Registration Service

TBD

## 

## Archive Server

1. Shall be used as the source for reporting.
2. Shall be used as a backup to the OTP database server
3. Shall be kept in sync with the OTP Server database close as possible.

## CRM Service

1. Shall be modified to support the MAC go to market info-structure.
2. Shall operate as a MAC run service.

# Definition of Terms

**Financial Instruction (FI)** – [banks](http://en.wikipedia.org/wiki/Bank), [building societies](http://en.wikipedia.org/wiki/Building_society), [credit unions](http://en.wikipedia.org/wiki/Credit_union), [trust companies](http://en.wikipedia.org/wiki/Trust_company), [mortgage loan](http://en.wikipedia.org/wiki/Mortgage_loan) companies, [Insurance companies](http://en.wikipedia.org/wiki/Insurance_company) and [pension funds](http://en.wikipedia.org/wiki/Pension_fund), [Investment Banks](http://en.wikipedia.org/wiki/Investment_Banks), [underwriters](http://en.wikipedia.org/wiki/Underwriting) and [brokerage firms](http://en.wikipedia.org/wiki/Brokerage_firm).

**Processor** – As it relates to the MAC business model are those transaction processing organizations that process transaction on behalf of the financial instructions.

**Merchant** – There are two type of merchants, and Online merchant and a Brick and Mortar merchant. Online merchants manly sales over the internet via a web site where as a Brick and Mortar merchant sales out of a store or physical location.

**Client** – The direct customer of MAC that is using MAC Services or has licenses or sub-licenses the products provided by MAC.

**User** or **End User** – The end user that has a phone and receives text messages from one or more of the MAC products.