CAT eAuthentication Admin Guide

Draft 13 December 2010

Mega AS Consulting Ltd.
E-mail: sales@megaas.com support@megaas.com
Tel: +972-3-6416406
WWW: http://www.megaas.com

Index

Preface

Mega AS Consulting Ltd is an R&D company working to provide secured, affordable and easy to deploy Identity Management and Strong Authentication. Identity Management is becoming a key issue for the continued evolvement and success of the Internet and LANs.

As the Internet enters more and more areas of our daily activities, so grows our dependency on its functionally and it is imperative to our way of life that our customers feel secure using the Internet. Our customers are the ones accessing our network services whether through the Intranet or Internet.

Mega AS defines two types of Internet service providers.

- Those that host their services on an in-house server
- Those that their services are hosted on a hosting service provider's server.

Accordingly we have developed two Identity Management types of solutions:

- The CAT AS (Authentication Server) is an off-the –shelf package for in-house installation
- The CAT eAuthentication service for hosted web sites.

CAT AS

The CAT AS can be purchased from Mega AS or its marketing partners and easily installed in-house. It is a powerful TFA OTP Strong Authentication and Identity management package that can be linked to any Radius protocol supporting device or software or integrated with any application using its API and Web Services. The CAT AS can be queried by remote servers and provide an eAuthentication service to other servers (under certain limitations).

CAT eAuthentication

The CAT eAuthentication service is a "SaaS" (Security as a Service) or "Cloud" service and is suitable for web sites requiring TFA OTP strong authentication. It is provided by ISPs and currently by Mega AS (as a Beta service).

If your web site is hosted and/or you don't want to maintain a costly identity management system on your server, but you still want your customers to feel secured with advanced and innovative TFA technology, than you should try our CAT eAuthentication service.

Today, any merchant web site that accepts credit cards, is getting its credit card verification and transactions service from a third party. We offer the same approach to Strong Authentication. Get your users verified by our CAT Authentication Server or in other words eAuthentication Service.

Offer your customers the option to upgrade their security. The customers can keep using the risky Fixed Password or upgrade and get a CAT to their cellular or PC that will generate a time based unique One Time Password (OTP). The TFA OTP is a proven methodology and accepted technology for preventing Identity Theft over the internet.

The CAT software is free and can be installed on most cellulars and PCs today including iPhones and Android (Google) cellulars.

How does it work

Most likely today, when users want to access your web site they are using a User ID and a Fixed Password (user details). At the server, your program checks the user details against the details held in a database and proceeds according to the results.

The eAuthentication does not change the process. The only change is that when the user details are checked your web site will use eAuthentication API to query the validity of the details. The program will proceed the same way with the eAuthentication result.

Web sites can have 2 approaches to adding new users:

- Every one can request to join the web site – in this case the web site has a Register web page where the new user enters his details and submits a request to be registered at the web site. The program adds the user to the database and may request to verify the user by sending an SMS or Email for final verification. Here again, the eAuthentication does not change the process it only replaces (or adds to) the register function. The web page will use the eAuthentication API to register the user at the eAuthentication service and next time this user tried to Login he will be found in the eAuthentication service and his OTP checked.

- Users are centrally managed and added manually by the Administrator. The administrator has access to the eAuthentication management system and can manage the web site details, users and logs.

CAT Tokens & Deployment

Whether you are using the CAT AS or CAT eAuthentication to secure the access to your server, your customers will need a CAT Token installed on their cellular or work station to generate the OTP (One Time Password).

Mega AS has CAT software for most cellular devices today and we work to extend our range of supported devices.

The CAT software for the cellular is more than a token. It is a multiple Site Accounts Tokens manager. You can add Accounts and manage them. Each Account is a different OTP token. So for example, let's say that Roger is a customer of yours and Roger's Bank is using the CAT AS and also his Internet Networking forum is using CAT eA to secure the members access. Roger will define 3 site accounts in his CAT software on his cellular - an account for your company, the bank and the forum. Each Account will show a different OTP at any given time.

Each Account and the authentication server share a secret. We call it – Secret Data. When adding a new Account in the CAT software using the CAT Menu, one has to enter the Secret Data value. This is a long string and it is entered once. For detailed instructions check the Mega AS web site.

To make the deployment process easier (getting the customer ready to use his/hers CAT software) for the customer, we provide multiple ways for delivering the CAT software to the customer cellular and adding the company Account.

Each company may choose the appropriate ways to deploy to each customer or to them all. Using the CAT API, the company can customize additional ways to deploy the CAT software that may be better used by their own customers.

The Basic option is to let the customer install the CAT on his cellular from the Internet like an installation of a cellular game. Once the CAT is installed on the cellular the customer will use

the Menu – Add Site Account Manually option to add a new account with the company details. In this case the customer has to have the Secret Data available to him. Usually the Secret Data is sent by other means to the customer – SMS, Email, Mail, or personally handed etc.

To save time and keying, the company can send an SMS to the customer's cellular with the download url. He still has to add the account manually.

Ultimately, using the CAT Identity Management system the admin can send to the customer an SMS with a personal download URL to a CAT package that already includes the company Account details.

There are also other ways. Please consult with us.

Requirements

The Hosted Web Site needs to have a fixed IP.

Signing for the service

First stage is to get in touch with our sales team: sales@megaas.com and get site identification number (**sid**). The **sid** will be needed when you customize your web site to use the eAuthentication APIs.

To open an eAuthentication account and get the **sid** you need to provide us with:

- The Web Site URL
- Web Site fixed IP
- Contact Person details: name, Email, Phone, country

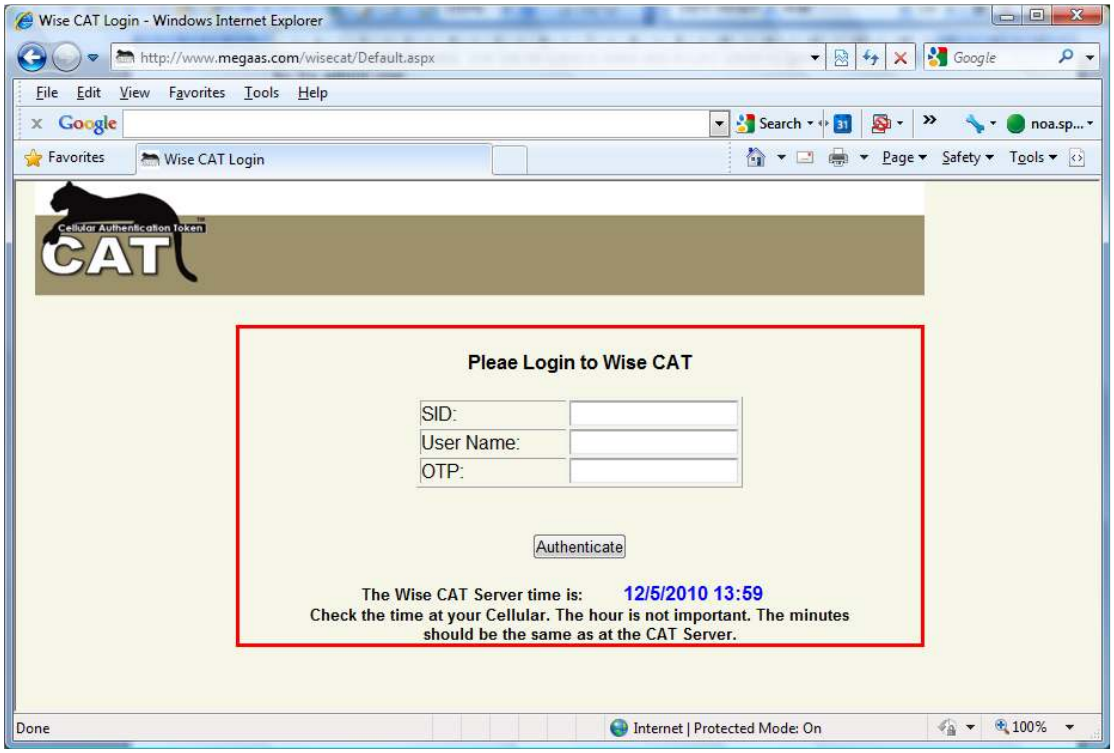
The **sid** is unique for each web site and should be kept in a safe place.

When your site is defined to the eAuthentication service a User ID **admin** is defined. You will get the user's Secret Data. The Secret Data is used with a CAT token to generate the OTPs for the **admin** user.

For more details about the CAT soft tokens go to our web site (www.megaas.com) and check the Products page.

The eAuthentication Management System

To access the eAuthentication management system go to: http://www.megaas.com/wisecat
Login to the management system using the admin user id and the OTP generated by your CAT token.



The system allows you to:

- Logout
- Manage the site details
- Manage the Users
- Import users from external file
- Check your site Logs
- Manage the site template messages
- Send SMSs (if the account has SMS credits)

Site details

Short Title:	megaas.com	Company:	Mega AS
Contact Name:	Arnnei	Email:	arnnei@megaas.
Phone:	1122333444	Country:	New Zealand
SD Length:	8	Otp Length:	6
Minus Grace:	3	Plus Grace:	3
Site IP:	12.222.13.223	Enabled:	True
Enable Registr:	True		
Disable After:	3 Login tries.	Enable After:	0 hours.
SMS Credits	99	Deploy Time	24 hours.
Default Jad	CATM1V2		
Send OTP Enabled:	True	Time Limit:	30 Minutes
Site notices can be sent to the Contact Email/Cell Phone (SMS requires credits):			
New Registration:	by Email	CAT Downloaded:	by Email
Id Disabled:	by Email	Site Updated:	by Email
SMS Service parameters	&serviceuser=aaaaa&servicepassw ord=bbbbb&servicesmtpid=ccccc		

Short Title – A sort name for the site. We suggest no more then 15 characters. When CAT tokens are deployed by SMS to new users this value is used as the Site name at the CAT token.

Company – full legal company name.

Contact name – the admin name

Email – the contact Email. The Email address will be used for automatic messages and notices generated by the system.

Phone – the contact Cellular phone number. This phone number will be used for automatic messages and notices generated by the system. Please do not enter + or blanks or leading zeros. The number should be: country code + phone number.

Country – choose the admin country of residence.

SD Length – the length of the Secret Data to be generated for each user.

OTP Length – the length of the OTP to be generated for this site.

Minus/Plus grace – clock miss match allowance. If the difference of the user Cellular clock minutes and server clock minutes is between the grace gap the OTP will be accepted.

Site IP – your web site fixed IP. This IP is checked when a Web Service is called.

Enabled – the status of your web site. Disabled site can not be logged to.

Enable Registration – allow the usage of the remote registration service. It means that the web site will allow users to Register to the web site and will use the register API.

Disable after – the number of consecutive login failures before disabling the user. Select 0 if you do not want to use this option.

Enable After – the number of hours after a user was automatically disabled to revive the user. Select 0 if you do not want to use this option.

SMS credits – the current number of SMS credits available to the site. SMS credits are bought from Mega AS. Contact the sales team sales@megaas.com

Deploy time – when a CAT was deployed to a user by SMS it is available for a limited number of hours from the time it was sent.

Default Jad – the name of the CAT token to be deployed to users by SMS.

Send OTP Enabled – True means the Web Service for sending OTP to an Identity is activated.

Time Limit – is the sent OTP time limit in minutes. By default, an OTP that was sent and not used in 30 minutes, expires.

New Registration notice – a short message will be sent to the administrator via the chosen vehicle notify him of any new user that registered to the site.

CAT Downloaded notice – a short message will be sent to the administrator via the chosen vehicle notify him of any deployed CAT that was received by the new registered user.

ID Disabled notice – a short message will be sent to the administrator via the chosen vehicle notify him of any new user was automatically disabled by the system.

Site Updated notice – a short message will be sent to the administrator via the chosen vehicle notify him when a change was made to the site, for example when SMS credits were added.

SMS Service Parameters – the parameters string will be added to the parameters that the system passes to the SMS Services Active Page. The system passes parameters like – the identity phone number and the SMS message text. The parameters in the sample above, are used to connect to your Mega AS SMS account provided by our SMS partners.

Manage the users

The users' management allows you to Check the users list, Add new users, Update users and Remove users.

Adding and or updating a user

SID:	1111111	User ID:	
Full Name:		Email:	
Phone:		Company:	Mega AS
Country:	New Zealand	Expiry Date:	< December 2020 >
User Type:	User	Authentication Type:	Otp
Enabled:	True	Send OTP by:	No
		Send OTP Password:	1234
Send Create Message:	Do not send	Select Message	Default Email
Encrypt SD with:			

Su	Mo	Tu	We	Th	Fr	Sa
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

SID – is your web site unique SID. For information only

User ID – a unique User ID. Single string of letters and numbers.

Full name – the user's full name.

Email – the user Email. This value will be used to send messages to the user.

Phone – the user Cellular number. This value will be used for SMS deployment and messages.

Company – the user's Company. By default it is the site Company.

Country – the user's country of residence.

Expiration date – the user's expiration date. After the expiration date he will not be able to Login to the web site.

User type – the admin can define another admin. The default is a regular user.

Authentication type – the type of password used for authentication. Can be:

- Otp – One Time Password generated using the CAT soft token.
- FixedPassword – fixed password string generated by the CAT system. You can not enter a fixed password value, the identity will have to use the value generated by the system.
- SentOTP – An OTP generated by the system that will be sent to the identity using the SentOTP2Identity Web Aervice.

Enabled – the user status. Disabled user can not login to the web site. A user may become disabled by the system if he failed a number of consecutive times to provide the correct password.

Send OTP By – When the identity Authentication Type is SentOTP, the user gets the OTP via SMS or Email as selected.

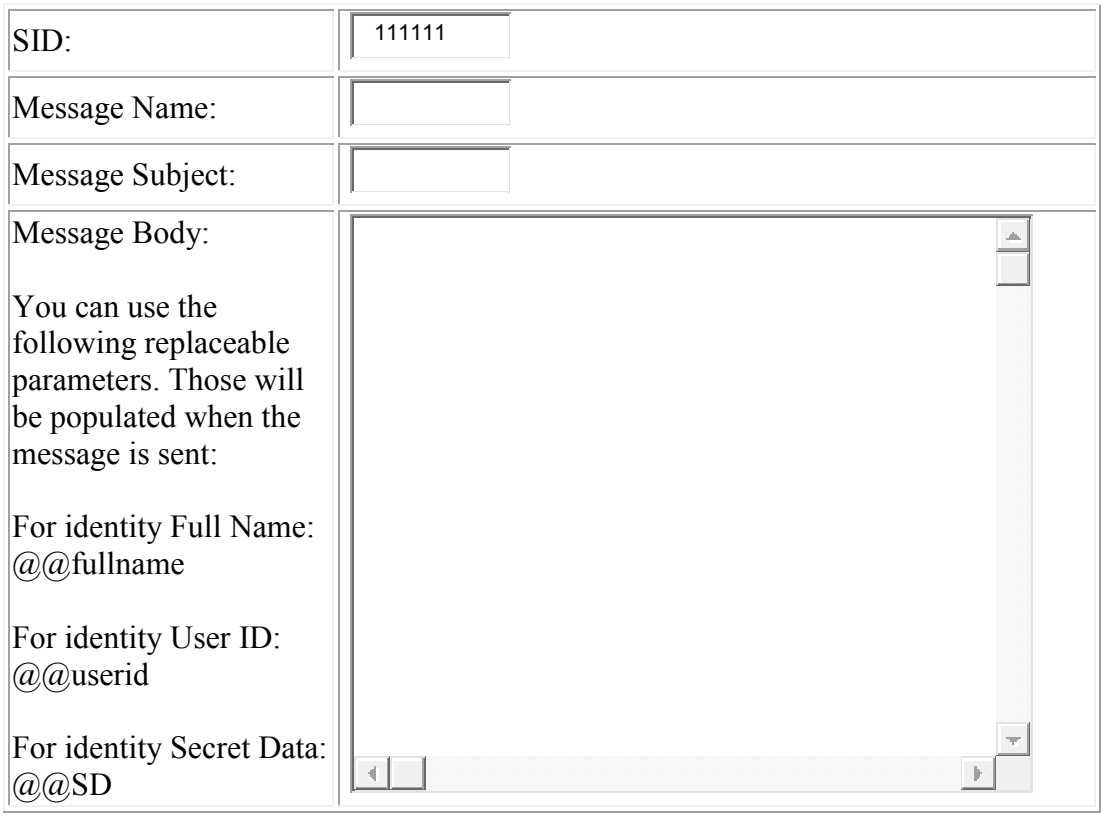
Send OTP Password – When the identity Authentication Type is SentOTP, the user has to request that an OTP is sent to him/her. This fixed password is used to authenticate the identity requesting the OTP. The administrator decides what the password is. The default value is 1234. It is up to the administrator to provide the identity with the Send OTP Password.

Send create message – send a predefined message to the new user by a chosen vehicle with details for the CAT token installation. When using SMS, the user gets a URL link for downloading his personal CAT token. Notice – currently deployment by SMS works for cellular types that support JAD type files download.

Select message – select the predefined template message to send to the user. There are 2 default messages. The admin can add/modify the templates. Notice – templates used for SMS should not exceed 150 characters.

Encrypt SD with – a password to encrypt the SD of the SMS deployed personal CAT token. This is additional security.

Manage the site template messages



Message name – this value is used for selecting the message. It should be a short text.

Message Subject – this value is used as Subject when the message is sent by Email.

Message body – the message content. Notice – the are a number of replaceable parameters that can be in the Message Body:

- For identity Full Name: @@fullname
- For identity User ID: @@userid
- For identity Secret Data: @@SD

These variables are replaced by the values prior to being sent.

For example, a template message such as:

Hi @@fullname, your CAT can be downloaded from: www.megaas.com/catr . After installation start the CAT and use the Menu to Add Site Manually.
Your Secret Data is: @@SD and your User ID is: @@userid.
Regards, Support Team

Will be sent as to new user jdoe:

Hi John Doe, your CAT can be downloaded from: www.megaas.com/catr . After installation start the CAT and use the Menu to Add Site Manually.
Your Secret Data is: 1q2w3e4a and your User ID is: jdoe.
Regards, Support Team

The eAuthentication Services

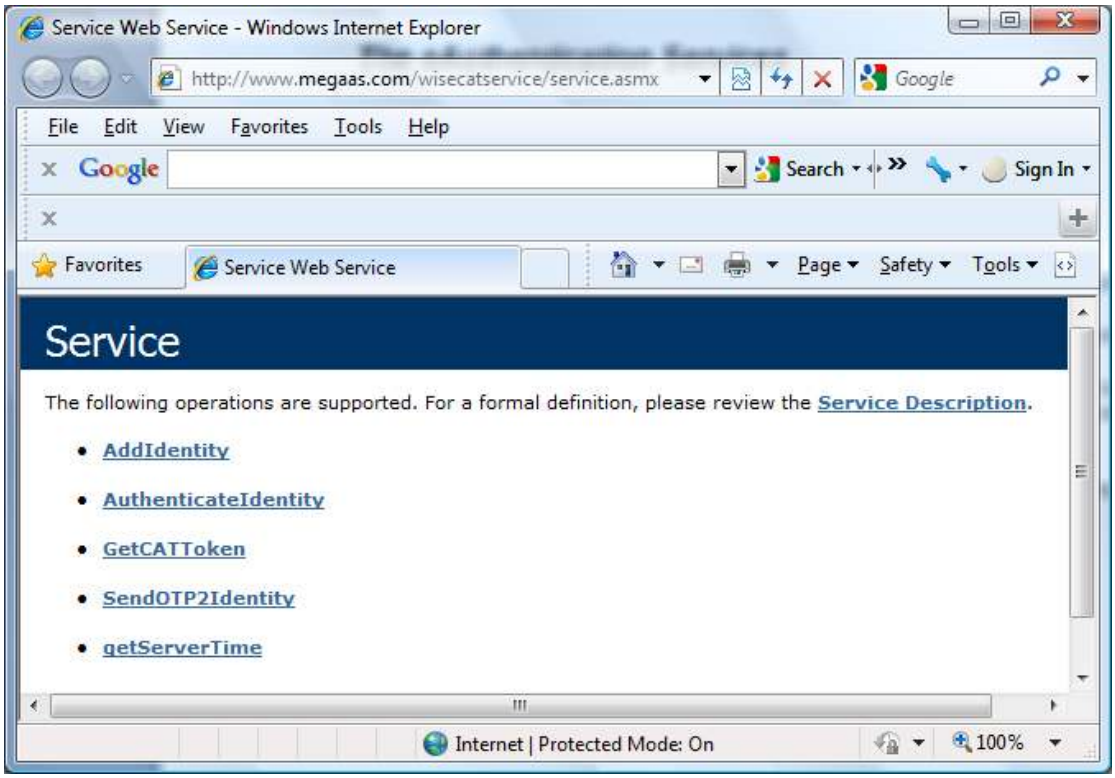
The following are .Net Web Service methods to be used in Web Pages:

- AddIdentity - this is the Registry service. Add a new Identity.
- AuthenticateIdentity – perform the Authentication query.
- GetCATToken – prepare values for the CAT token, Is not for public use.
- SendOTP2Identity – generate an OTP and SMS or Email it to the identity.
- getServerTime – get the current Server Time. Used to let the users compare with their Cellular clock. Make sure the deviation is not over the grace allowed.

The Web Services parameters correspond to the same eAuthentication Management System pages.

You can see the web service at:

http://www.megaas.com/wisecatservice/service.asmx



AddIdentity

http://www.megaas.com/wisecatservice/Service.asmx?op=AddIdentity

The values are similar the eAuthentication Management System - the Add new Identity option

Parameter	Value	
txtSid:		Your site unique sid
txtUserid:		The identity User ID
txtFullName:		First & Last name
txtEmail:		Valid Email
txtCompany:		Company name
txtPhone:		Valid phone number no leading + or 0
pdEnabled:		True / False
pdAuthenticationType:		Otp, FixedPassword or SentOTP
pdOTPIsDeliveredBy:		SMS or Email When Auth Type is SentOTP
txtCountry:		Identity Country
pdSendMessageBy:		Send the identity a new user Email or download url with SMS
pdMessageTitle:		Use this message format
txtEncPassword:		Encrypt the downloaded CAT

Service returns XML. On success:

```
<?xml version="1.0" encoding="utf-8" ?>
<string xmlns="http://wisecat.services.com/">Success</string>
```

On failure:

```
<?xml version="1.0" encoding="utf-8" ?>
<string xmlns="http://wisecat.services.com/">Failed. User ID already exists.</string>
```

AuthenticateIdentity

http://www.megaas.com/wisecatservice/Service.asmx?op=AuthenticateIdentity

Parameter	Value	
sid:		Your site unique sid
userid:		The authenticated User ID
otpassword:		The CAT generated OTP

Service returns XML:

On success:

```
<?xml version="1.0" encoding="utf-8" ?>
<boolean xmlns="http://wisecat.services.com/">true</boolean>
```

On Failure:

```
<?xml version="1.0" encoding="utf-8" ?>
<boolean xmlns="http://wisecat.services.com/">false</boolean>
```

SendOTP2Ideentity

http://www.megaas.com/wisecatservice/Service.asmx?op=SendOTP2Identity

Parameter	Value	
sid:		Your site unique sid
userid:		The identity User ID
usersmspassword:		The identity Send OTP Password set by the administrator

Service returns XML:

On success:

```
<?xml version="1.0" encoding="utf-8" ?>
<boolean xmlns="http://wisecat.services.com/">true</boolean>
```

On Failure:

```
<?xml version="1.0" encoding="utf-8" ?>
<boolean xmlns="http://wisecat.services.com/">false</boolean>
```

getServerTime

http://www.megaas.com/wisecatservice/Service.asmx?op=getServerTime

Service returns:

```
<?xml version="1.0" encoding="utf-8" ?>
<string xmlns="http://wisecat.services.com/">6/15/2010
13:55:21.1621250</string>
```

Templates for calling the Services

The Services were developed using ASP.NET.

Calling a service using ASP 2.0 template.

AuthenticateIdentity

```
      Dim xmlhttp
      Dim DataToSend
      DataToSend="sid=" & sid & "&userid=" & userid & "&otpassword=" & otpassword

      Dim postUrl
      postUrl = "http://www.megaas.com/wisecatservice/service.asmx/AuthenticateIdentity"

      Set xmlhttp = server.Createobject("MSXML2.XMLHTTP")
      xmlhttp.Open "POST",postUrl,false
      xmlhttp.setRequestHeader "Content-Type","application/x-www-form-urlencoded"
      xmlhttp.send DataToSend

      Dim resp
      resp = xmlhttp.responseText

      '--------------------------------------
      if (instr(resp,"System.Exception") > 0) then
            resp = replace(resp,"System.Exception:","")
            resp = mid(resp,1,instr(resp,"at") - 1)
      end if
      Session.Timeout = 30
      '----------------------------------------------
    'Check the verification result and move to the next page.
        If instr(resp,"true") > 0 then
            Session("isvalid") = "Y"
            Session("LoginName") = userid
            Response.redirect(SuccessURL  + "?msg=You have successfuly Logged into Mega
AS Server")
        Else
            Session("isvalid") = "N"
            Response.redirect(FailURL & "?msg=" & resp)
        End If
```

Calling a service using PHP template

The following is a template for calling the `AuthenticateIdentity method`.

```
<?php
  // create a connection to the local host mono .NET pull back the
wsdl to get the functions names
  // and also the parameters and return values
  $client = new
SoapClient("http://www.megaas.com/wisecatservice/service.asmx?wsdl",
    array(
      "trace"      => 1,           // enable trace to view what is
happening
      "exceptions" => 0,           // disable exceptions
      "cache_wsdl" => 0)           // disable any caching on the
wsdl, encase you alter the wsdl server
  );

  // get a response from the WSDL zend server function getQuote for
the day monday
  print_r( $client->AuthenticateIdentity(array("sid" => "16245",
"userid" =>"Arnnei", "otpassword" =>"61C026")));

  // display what was sent to the server (the request)
  echo "<p>Request :".htmlspecialchars($client->__getLastRequest())
."</p>";
  // display the response from the server
  echo "<p>Response:".htmlspecialchars($client-
>__getLastResponse())."</p>";
?>
```

The results:

stdClass Object ([AuthenticateIdentityResult] => 1)

Request :<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://wisecat.services.com/"><SOAP-ENV:Body><ns1:AuthenticateIdentity><ns1:sid>16245</ns1:sid><ns1:userid>Arnnei</ns1:userid><ns1:otpassword>61C026</ns1:otpassword></ns1:AuthenticateIdentity></SOAP-ENV:Body></SOAP-ENV:Envelope>

Response:<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><AuthenticateIdentityResponse xmlns="http://wisecat.services.com/"><AuthenticateIdentityResult>true</AuthenticateIdentityResult></AuthenticateIdentityResponse></soap:Body></soap:Envelope>

Notice that the Response result can be parsed from:
<AuthenticateIdentityResult>true</AuthenticateIdentityResult>

The main thing is to check with the Web Server administrators that the PHP SOAP extension is enabled at the server.

AddIdentity

```
	'-------------------------------------------------------------------------------
	' Build the registration process
	'-------------------------------------------------------------------------------
	'Valid values:
	'pdEnabled = true / false
	'pdAuthenticationType = Otp / FixedPassword
	'pdSendMessage = None / byEmail / bySMS (for SMS the site has to have SMS credits)
	'pdMessageTitle= None / Message title (if title is wrong the send will fail)

	Dim DataToSend
	DataToSend="txtSid=" & sid & "&txtUserid=" & userid & _
	"&txtFullName=" & username & _
	"&txtEmail=" & email & _
	"&txtCompany=" & company & _
	"&txtPhone=" & countrycode & phone & _
	"&pdEnabled=true" & _
	"&pdAuthenticationType=Otp" & _
	"&txtCountry=" & countrycode & _
	"&pdSendMessage=" & sendby & _
	"&pdMessageTitle=" & messagetitle  & _
	"&txtEncPassword=" & txtEncPassword

	Dim postUrl
	postUrl = "http://www.megaas.com/wisecatservice/service.asmx/AddIdentity"

	resp = GetService(postUrl, DataToSend )
	Session.Timeout = 30

	'-------------------------------------------------------------------------------
	' Check the registration rc
	'-------------------------------------------------------------------------------

	If instr(resp,"Success") > 0 then
		Session("isvalid") = "true"
		Response.redirect(successurl  + "?msg=Your registration details were sent to
you " & sendby)
	Else
		Session("isvalid") = "false"
		Response.redirect(failurl & "?msg=" & resp)
	End If
```

SMS / Email Options

The eAuthentication provides SMS or Email messaging capabilities when certain events occur. The admin can set up the eAuthentication site account whether to receive the messages by Email or SMS. To receive messages by SMS the account has to have SMS credits. SMS credits can be purchased from Mega AS Ltd. Contact us for prices.

The following events will generate a message to the admin user Email or Phone number.

- Your eAuthentication account was changed
- Users list was updated or new users added
- User was added or removed

The following will generate a message to a user Email or Phone number (depends on the decision of the admin)

- When the user is added, his CAT details can be sent by Email or a personal CAT Download URL can be sent by SMS. Sending a Download URL will work for certain cellular types, for example – Symbian. We are working to extend that capability to a wider range of cellular types.

Support

You can contact our support by Email: support@megaas.com and we will respond soon as possible.