SOLUTIONS OVERVIEW: TOKEN AUTHENTICATION

Overview

With our solutions, we aim to minimize barriers to learning and when a user has to remember security credentials for multiple systems, it can create a barrier and reduce utilization.

To help with this challenge, we can configure Token Authentication. Many clients use an intranet portal or another web-based application that can be configured to work with a BizLibrary service that will provide a Single Sign-On like experience.

Goals

- Reduce barriers for users.
- The client intranet portal is the controlling entity for identifying the current user and authentication pattern.
- Implement a solution that utilizes industry accepted best security practices.

Example Flow

- User A goes to their intranet site and they are presented with a link to the BizLibrary learning platform.
- The user clicks on the link.
- The link goes to a custom location on the intranet site that interacts with the BizLibrary service.
- The intranet site redirects the user to a unique URL with a token for access.
- The learning platform checks the token and authenticates the user.

The client's system is responsible for:

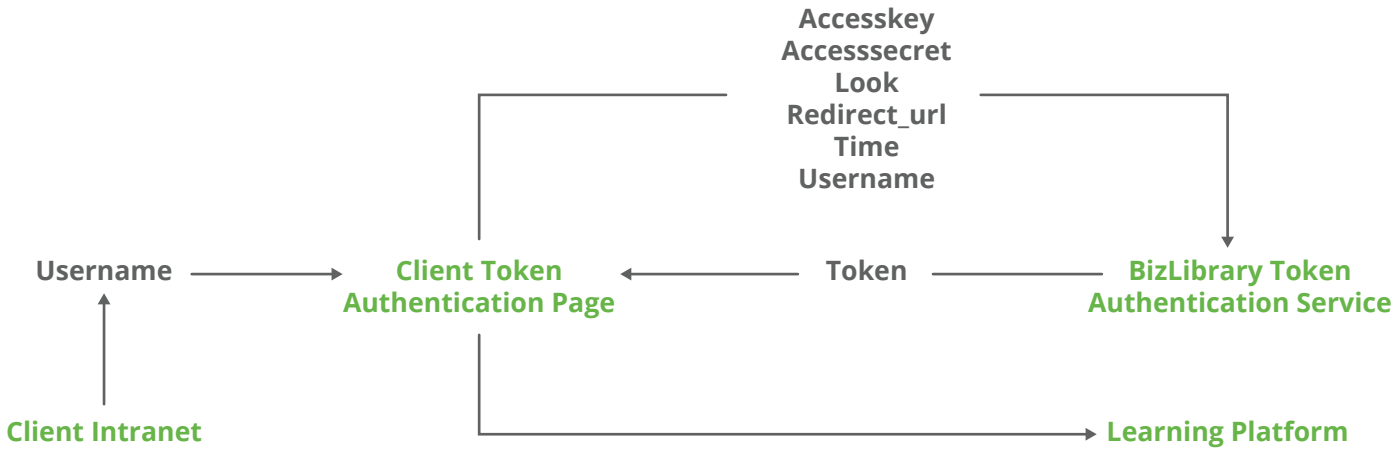
- Identifying the current user.
- Implementing code and functions that interact with the BizLibrary service.
- Configuring access keys and access key changes according to BizLibrary security standards. If configured clients do not comply, the access keys will be disabled.

BizLibrary will:

- Provide clients with example code in C# ASP.NET and PHP that will interact with the BizLibrary service.
- Request changes to the client access keys according to BizLibrary security standards.
- Trust the client application to determine the current user and allow the user access.
- Protect against multiple use of the same authentication token.
- Only interact with client applications via HTTPS with the latest generally accepted web security standards.

Detailed Description

This section intended for the client development teams.



The token authentication service requries the following fields to be posted when submitted:

Field Name	Description
accesskey	This is a unique identifier used to identify the client accessing the utility • Example: "TESTSSO"
accesssecret	This is a predetermined key that is known only by the communicating systems • Example: "4FG2BDA9C90AASDFG74934AC2F5DFAAD"
look	This is the look used for display • Example: "btl"
redirect_url	This designated the landing page upon a successful login • "/Site/Home"
time	This represents the time of the request. The values is in # of seconds from the epoch time (1/1/1970) • Calculated by requesting server
username	This is the username of the user requesting access • Determined and provided by requesting server (LDAP, Application User, etc.) • Client can test this by hard coding a test user (be sure to prefix "cn\\" to the username for example)

Upon successful login, the user will be redirected to the specified (“redirect_url”) page. If this value is not specified, they will be redirected to their default landing page.

If there is an error processing the request, the application will throw a 401 – Access Denied error. To troubleshoot this error, the user can attempt to login to the site directly (http://www.companycollege.com/clientlook) or have an administrator check to ensure that the username is active and exists in the system.

Client Configuration Values

Field Name	Description
accesskey	
accesssecret	
look	
redirect_url	/Home

Additional Information

Example code (written in ASP.NET C#)

```
<%@ Page Language="C#" AutoEventWireup="true" %>

<%@ Import Namespace="System.Collections.Specialized" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.Net.Security" %>
<%
DateTime epoch = new DateTime(1970, 1, 1);
DateTime now = DateTime.UtcNow;
TimeSpan sinceEpoch = now.Subtract(epoch);
string lmsSSOUrl = "https://lms.bizlibrary.com/Services/SSO";
NameValueCollection formData = new NameValueCollection();
formData["accesskey"] = "TESTSS0";
formData["accesssecret"] = "512300AA59AD4DXYZ63226728AB575B";
string username = Page.User.Identity.Name;
if (username.IndexOf("\\") > -1)
{
        username = username.Substring(username.IndexOf("\\") + 1);
        username = username;
}
formData["username"] = username;
formData["look"] = "look";
formData["redirect_url"] = "//Home";
formData["time"] = sinceEpoch.TotalSeconds.ToString();
using (WebClient webClient = new WebClient())
{
        try
        {
                byte[] responseBytes = webClient.UploadValues(lmsSSOUrl, "POST", formData);
                Response.Redirect(System.       Text.Encoding.UTF8.GetString(responseBytes));
                }
                catch (WebException exception)
                {
                        string responseText;
                                using (var reader = ne
                        System.IO.StreamReader(exceptionResponse.GetResponseStream()))
                {
                        responseText = reader.ReadToEnd();
                }
                Response.Write(responseText);
            }
        }

%>
```

Additional Information

Example code (written in PHP)

```
<?php

//set variable "live" = 1 for production, 0 to debug the response and not redirect;
$live = 1;

$lmsSSOUrl = "https://lms.bizlibrary.com/Services/SSO";

$fields = array(
                'accesskey' => 'ABCSSO',
                'accesssecret' => "XXXXXXXXXXXXXXXXXXXXXXXXX",
                'username' => $row_user['account_username']."@Test.com",

                /*
                or use authenticated user
        an authenticated user on your server 'username' => $_SERVER['AUTH_USER'];

*/

                'look' => 'test',
                'redirect_url' => '/Home', 'time' => time()

);
$ch = curl_init();
foreach
($fields as $key=>$value)
                { $fields_string .= $key.'='.$value.'&'; }
//set the url, number of POST vars, POST data
curl_setopt($ch, CURLOPT_URL, $lmsSSOUrl);
curl_setopt($ch, CURLOPT_POST, count($fields));
curl_setopt($ch, CURLOPT_POSTFIELDS, $fields_string);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
//execute post
$result = curl_exec($ch);

if($live == 1){
        //redirect user to the response result URL
        header("Location: $result");
}else{
        echo "Response from server: $result <br /><br />"; print_r($fields);
        echo 'Server info <br /><br />'; print_r($_SERVER);
        echo 'Session info <br /><br />'; print_r($_SESSION);
}
//close connection
curl_close($ch);
?>
```