KFC Single Sign-On Portal

Launch

Developer Implementation Documentation

CECS 491B, Sec 11

April 22, 2019

Julian Poyourow
013466646

Revision History

Date	**Version**	**Description**
4/22/19	1.0	First draft.

Table of Contents

1. SSO Launch Request

You'll need to register an app with the SSO through the app registration interface.

Then you'll be able to launch your app from the dashboard.

The incoming payload to your application's launchURL will be a POST request, and will be in the following format:

```
{
  email: "julianpoyo+22@gmail.com",
  signature: "4T5Csu2U9OozqN66Us+pEc5ODcBwPs1Idaq2fmBqtfo=",
  ssoUserId: "0743cd2c-fec3-4b79-a5b6-a6c52a752c71",
  timestamp: "1552766624957",
}
```

You'll need to hash that payload using the SignatureService included with SSO, and compare the resultant hashes. For example, the SharedSecret for that payload is:
D078F2AFC7E59885F3B6D5196CE9DB716ED459467182A19E04B6261BBC8E36EE
You'll need to sign the request and compare the hashes.
The string to sign for that particular request looks like this:
"email=julianpoyo+22@gmail.com;ssoUserId=0743cd2c-fec3-4b79-a5b6-a6c52a752c71;timestamp=1552766624957;"

"email=luis8louis@yahoo.com;ssoUserId=0f3d85de-15e8-488e-819b-613891e59178;timestamp=1556148198953;"

If you put that string through your own HMAC SHA256, you'll get a matching signature as is what is contained above.

The resulting signature must be in base64 format.

2. Validation Steps and Protocol

When you receive a request to your launchURL:

1. Concatenate those parameters key=value separated by semicolons (as I mentioned above with that string to sign). Make sure the order is sorted **by key, alphabetically**

2. Run it through HMAC SHA256 with your shared secret
3. Verify that the signature the SSO sent matches the signature that HMAC SHA256 output
4. Create if not exists the user in your system by the provided SSO ID
5. Generate that user a new token string and store it in the clients browser, or redirect them to your frontend URL with the token as a query parameter for your own frontend to digest.
6. Return a redirect status code

3. Useful Tools

You can play around with HMAC SHA256 here:

https://www.freeformatter.com/hmac-generator.html

But keep in mind that site outputs HEX. You can convert hex to base64 here:

http://tomeko.net/online_tools/hex_to_base64.php