USAJOBS

Technical Guide to USAJOBS Single Sign-On for Job Seekers

FROM:
Office of the Chief Information Officer
U.S. Office of Personnel Management
1900 E Street NW
Washington, DC

August 18, 2013

Version 1.1

Revision Sheet

Release Number	Date	Revision Description
3.9	08/18/2013	Initial draft guidance describing data interchanges for OPM's USAJOBS.
4.0	10/17/2013	Update overview to indicate test scripts will not be provided.

Table of Contents

Goals

Since the deployment of USAJOBS 3.0, it has been a goal of the program to deploy a single sign-on (SSO) solution for job seekers to simplify their user experience and to continue to improve the integration between USAJOBS and its vendor partners. Prior to the implementation of SSO, job seekers were required to maintain User IDs and Passwords for USAJOBS and each Talent Acquisition System vendor they interacted with, to apply for job opportunities. By implementing SSO, USAJOBS has identified the following positive outcomes:

- Eliminate Redundant Logins across the Federal Job Applicant process
- Provide an end-to-end Hiring Authentication Experience to Job Seekers
- Eliminate Redundant Account Management for Seekers throughout the Talent Acquisition System Life Cycle
- Enhance Data Security for the Talent Acquisition System Supply Chain in the Federal Government.

Overview

To implement these goals, a comprehensive approach to Seeker authentication needed to be designed and implemented. The job seeker SSO capabilities needed to expand well beyond just the job application process to ensure Seekers realized all identified goals.

At the foundation of job seeker SSO, a new Identity Management Service was developed for USAJOBS and all supporting partner solutions, which is login.usajobs.gov. This new Identity management service will not only support authentication of job seekers for vendor integration, but will also be leveraged for Seeker authentication to USAJOBS itself. With SSO activated:

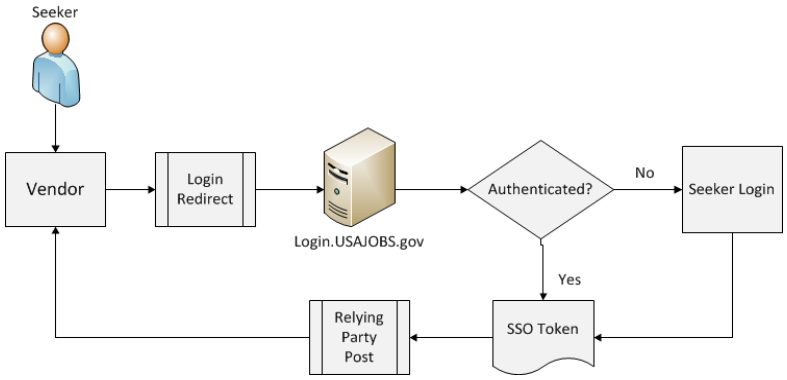
- All authentication is now done via this service.
- USAJOBS calls login.usajobs.gov to authenticate the job seeker when they desire to login
- When a vendor wishes to authenticate the job seeker, they will redirect to login.usajobs.gov to validate the authentication OR have the job seeker login and authenticate (if outside the application process)

The design for Seeker SSO leveraged multiple design use cases and supports a Federated SSO Design. By taking this approach, the use cases required that the implementation of Seeker SSO:

- Support the current Application Process and eliminate secondary vendor logins
- Support new authentication outside of the Application Process for requirements like Assessments, Onboarding, Suitability, etc. with agency or Talent Acquisition System (TAS) selected vendors.

Seeker SSO leverages a common architecture approach. The common architecture leverages a single foundation built on the WS-Federation Architecture. This architecture is an Open Standard supported by OASIS (Organization for the Advancement of Structured Information Standards):

- Seeker SSO leverages the Federated SAML 2.0 Token.
- Login.USAJOBS.gov is the Federated Identity Management Service (to include USAJOBS). It allows the vendor to authenticate the job seeker with USAJOBS at any point in the process where authentication is required.



Accessing the SSO Framework

Access to SSO will be tightly controlled. As each vendor appreciates, it is critical that the integration between each vendor and USAJOBS must be stable and validated. A system control has been established that allows USAJOBS to configure SSO access by Vendor, by Environment (UAT or Production). It is critical to understand that once SSO is activated for a vendor, in a given environment, that all USAJOBS system behavior and integration with that vendor will reflect the configuration. A vendor cannot process in both the current mode and SSO simultaneously. For example, if Vendor A wishes to begin testing with USAJOBS in the UAT environment, the configuration will be changed for that vendor to operate only in SSO mode. The configuration can be switched back if required, but the number of changes should be minimized if possible.

Access to the SSO Capabilities is provided according to two sets of access requirements:

Existing TAS Vendors

As each TAS Vendor prepares to migrate to UAT for SSO, they should fill out the UAT Registration Form which has additional questions and submit the request to the access@opm.gov email address. With that request, a ticket will be established and the USAJOBS team will work with the vendor to set the date and time that the configuration change will occur. As part of this process, USAJOBS will issue the vendor the appropriate credentials that will be unique to their deployment in UAT. If the TAS vendor needs to perform parallel testing and development with SSO and non-SSO configurations, a separate office and SIF token will need to be created.

Once the configuration change is made, the USAJOBS team will provide the vendor with a scorecard to verify that their SSO implementation is working properly. The USAJOBS team will work with the vendor to ensure all tests are properly passed and that the integration is working seamlessly.

Once testing is confirmed for that vendor, USAJOBS will work with the vendor to schedule the production go live date and time. At that time, the production credentials will be published to the vendor as well.

New Vendors

Each new vendor that interacts with USAJOBS, must submit the UAT Request Form, located on schemas.usajobs.gov. Once the form is submitted, the USAJOBS team will validate the request with the sponsoring agency, establish a Vendor ID, Staffing Integration Framework (SIF) Authenticate Token and configure that vendor for access to the UAT Test environment only.

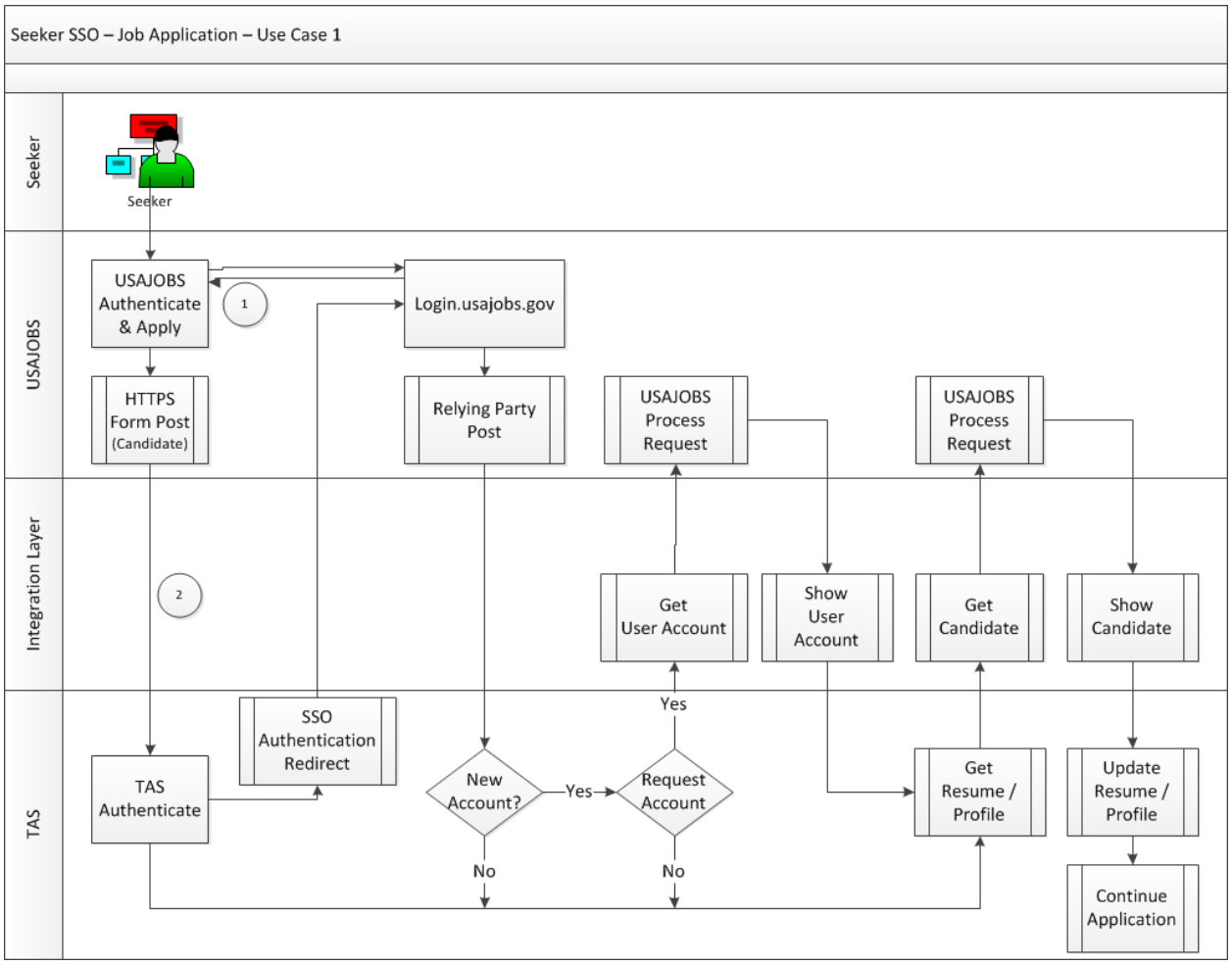
Once the configuration is completed, the USAJOBS team will provide the vendor with a scorecard to verify that their SSO implementation is working properly. The USAJOBS team will work with the vendor to ensure all tests are properly passed and that the integration is working seamlessly.

For new vendors to gain access to the production environment, they will need to work with the USAJOBS Security team to provide proof of their Government Certified Security Assessment & Authorization (SA&A) and Federal Information Security Management Act (FISMA) Compliance. Once compliance is certified and the security office has granted production access approval, USAJOBS will work with the vendor to schedule the production go live date and time. At that time, the production credentials will be published to the vendor as well.

Implementing Seeker SSO – The Application Process

Within the application process, the initial authentication of the job seeker will occur with USAJOBS. When the job seeker is authenticated, they will complete their application(s) and be directed to the TAS, in similar fashion as originally deployed with Release 3.0. But, how USAJOBS interacts with the TAS will change slightly and the TAS is expected to authenticate the job seeker differently than done today. Below are the new steps and process flow that apply under SSO.

Application Process Overview



Seeker Authentication

The primary difference from the initial Seeker authentication on USAJOBS in Release 3.0 and now under SSO, is that USAJOBS will leverage the same process as all vendors. Seeker authentication will universally be completed via the login.usajobs.gov service. The following steps outline the process USAJOBS will follow:

- Step 1: Seeker accesses a part of USAJOBS which requires authentication.
- Step 2. USAJOBS no longer redirects the job seeker to the login page, rather, the job seeker is redirected to login.usajobs.gov with several query parameters.

QueryString

Name	Value
wa	wsignin1.0
wtrealm	https://www.sqa.usajobs.gov/
wctx	rm=0&id=passive&ru=%2fApplicant%2fMyAccount%2fHome
wct	2013-04-29T01:11:55Z

  - The query string parameter wtrealm specifies the relying party's URL which is validated.
  - The query string parameter wctx includes the return URL which the relying party will direct the user to.

- Step 3: Seeker authenticates on login.usajobs.gov.
- Step 4: Login.usajobs.gov does a post back to the relying party with the SAML Token to communicate if the Login was successful or failed:

Body

Name	Value
wa	wsignin1.0
wresult	<trust:RequestSecurityTokenResponseCollection xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512"><trust:RequestSecurityTokenResponse Context="rm=0&id=passive&ru=%2fApplicant%2fMyAccount%2fHome"><trust:Lifetime><wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2013-04-29T01:12:09.300Z</wsu:Created><wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2013-04-29T01:42:09.300Z</wsu:Expires></trust:Lifetime><wsp:AppliesTo
wctx	rm=0&id=passive&ru=%2fApplicant%2fMyAccount%2fHome

- Step 5: The relying party validates the Token with the public key provided by USAJOBS
  - The relying party extracts the claims which includes:

    LastName, GivenName, Email, SessionID
  - The relying party then sets their session to authenticated.

USAJOBS Notification to TAS

Once the Seeker has logged into USAJOBS and been authenticated, the SSO Token and SSO Session have been established. It is important to note that the SSO Token and SSO Session are independent from the USAJOBS Authenticate Token and Session ID provided in the HTTP Form Post. The SSO Token, with embedded SSO Session, will be passed with the cookie when the job seeker is redirected from USAJOBS to the TAS.

Like today, the HTTP Form Post will be generated to the TAS. But, the Form Post generated to the TAS redirecting the job seeker to them, will no longer include the Candidate ID. However, a new field, SessionID will be passed. As the Candidate is redirected to the TAS, they will not have a SSO Token and SSO Session that has been Authenticated for the job seeker / session in the TAS.

```
form action="" method="post" name="frmApplyPost" id="frmApplyPost"
class="grid_16"><input id="PositionOpening.DocumentID"
name="PositionOpening.DocumentID" type="hidden" value="200013" />
<input id="Candidate.AlternateDocumentID" name="Candidate.AlternateDocumentID"
type="hidden" value="200013" />
<input id="ReturnURL" name="ReturnURL" type="hidden"
value="https://my.usajobs.gov/Apply/ApplyReturn.aspx" />
<input id="DocumentInfo" name="DocumentInfo" type="hidden"
value="7115073|COVER|docx|Test Cover Letter,7116514|SECURE_RESUME|docx|Uploaded
Resume 1"/>
<input id="SessionTicket" name="SessionTicket" type="hidden" value="d143eb46-8489-4480-
9149-9145e3888818" />
<input id="SessionID" name="SessionID" type="hidden" value="292b6bcb-2e59-4b54-945c-
f1112c9e96e4" />
</form>
```

IMPORTANT: The variables in the Form Post should be saved prior to the Redirect to login.usajobs.gov. Although the Candidate ID will no longer be passed, it will be match the form data when the user is redirected by using the Session ID which is passed in the SAML Token.

The TAS will redirect the job seeker to login.usajobs.gov. With the redirect, the cookie and supporting SSO Token/Session will be part of the redirect.

- Login.usajobs.gov will read the SSO Token and leveraging the SSO Session will authenticate the job seeker based on the SSO Session established by USAJOBS.
- The updated SSO Token will be posted back to the Relying Party ID as the job seeker is redirected back to the TAS.
- The TAS will then validate the Token with the public key provided by USAJOBS.
- The TAS will leverage the Claims in the Token to establish their session as authenticated.

Within the SSO Token, the following Claims will be provided:

```
<AttributeStatement>
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/lastname">
        <AttributeValue>Jones</AttributeValue>
</Attribute>
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
        <AttributeValue>MyFirstName</AttributeValue>
</Attribute>
<Attribute
Name="http://schemas.microsoft.com/accesscontrolservice/2010/07/claims/identityprovider">
        <AttributeValue>login.usajobs.gov</AttributeValue>
```

```
</Attribute>
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
        <AttributeValue>MyFirstName.Jones@opm.gov</AttributeValue>
</Attribute>
<Attribute Name="http://schemas.usajobs.gov/identity/2013/04/claims/nameid">
        <AttributeValue>100000120</AttributeValue>
</Attribute>
<Attribute Name="http://schemas.usajobs.gov/identity/2013/04/claims/sessionid">
        <AttributeValue>292b6bcb-2e59-4b54-945c-f1112c9e96e4</AttributeValue>
</Attribute>
</AttributeStatement>
```

NOTE: Nameid is the Candidate ID.

Post Authentication Processing

Once the SSO Token has been received and validated, the TAS now has several different Options or paths it can take. As each TAS is designed differently, USAJOBS recognizes that some TAS vendors will need to internally establish an account or update the existing account before creating the application itself. Others will desire to simply leverage the GetCandidate Data to accomplish the same requirements. To support those vendors that need to establish or update an account before getting the application data, two new BODS were added to the SIF.

- BOD GetUserAccount. The GetUserAccount BOD allows the TAS to request the base account data used to establish or update a base account in their system. Using the USAJOBS SessionID, the GetUserAccount will request this information from USAJOBS.
- BOD ShowUserAccount. Upon receipt of the GetUserAccount, the request will be validated by USAJOBS using the standard SIF Security processes. USAJOBS will return the ShowUserAccount with the status of the request and for Accepted transactions, the corresponding data for the job seeker account will be returned.

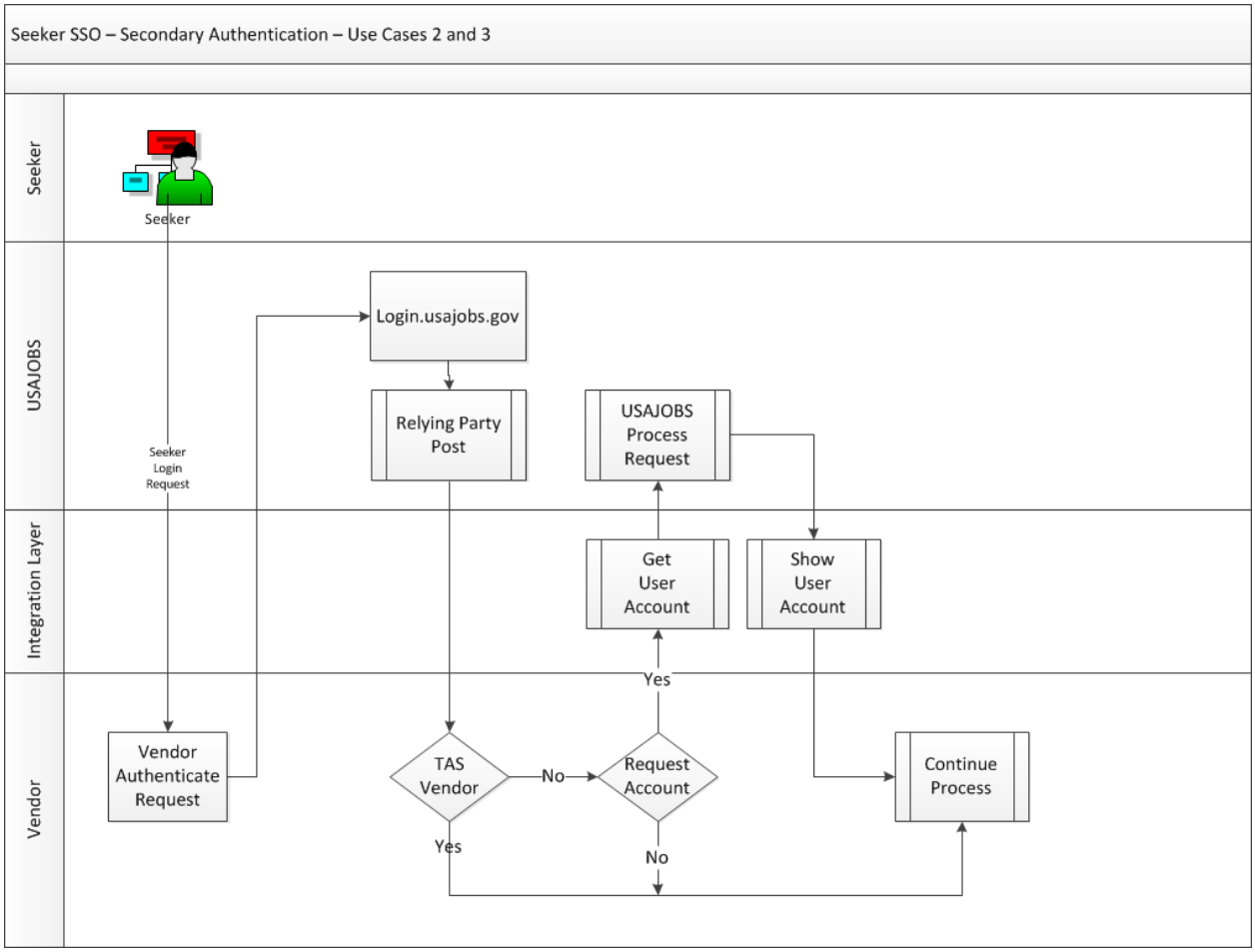
The TAS would then continue with GetCandidate as is done today to retrieve the application data. Again, the TAS can bypass GetUserAccount and retrieve the same information from the GetCandidate, if appropriate.

Implementing Seeker SSO – Secondary Authentication

Implementing Seeker SSO is a paradigm shift for how job seekers are authenticated for both USAJOBS and TAS vendors. To truly implement the goals of SSO, the use of vendor specific User Ids and Passwords needs to be addressed through the Talent Acquisition System lifecycle. Applying for jobs many times involves far more than just interactions with USAJOBS and the Agency TAS. Many times, additional applications are involved to support processes and requirements supporting Assessments, Suitability, Onboarding and other needs.

To support these additional requirements, Seeker SSO was designed to allow job seeker authentication outside of the application process as well.

Secondary Authentication Overview



Seeker Authentication

For authentication of a job seeker outside of the application process or as a secondary process within the application, the vendor's solution will initiate the authentication. It should be noted that if a job

seeker was required to take an assessment as part of the application process, it would be no different than a vendor requesting authentication after the application process was completed.

The following steps outline the steps a vendor will take:

- Step 1: Seeker accesses a vendor's solution to login and requires authentication.
- Step 2. Vendor solution would redirect the job seeker to login.usajobs.gov with several query parameters.

QueryString

Name	Value
wa	wsignin1.0
wtrealm	https://www.sqa.usajobs.gov/
wctx	rm=0&id=passive&ru=%2fApplicant%2fMyAccount%2fHome
wct	2013-04-29T01:11:55Z

  - The query string parameter wtrealm specifies the relying party's URL which is validated.
  - The query string parameter wctx includes the return URL which the relying party will direct the user to.
- Step 3: Seeker authenticates on login.usajobs.gov. Because the redirect does not contain the SSO Token or Session ID with the redirect, the job seeker will be queried for their USAJOBS UserID and Password on the Login Page.
- Step 4: Login.usajobs.gov does a post back to the relying party with the SAML Token to communicate if the Login was successful or failed. The updated SSO Token will be posted back to the Relying Party ID as the job seeker is redirected back to the TAS.

Body

Name	Value
wa	wsignin1.0
wresult	<trust:RequestSecurityTokenResponseCollection xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512"><trust:RequestSecurityTokenResponse Context="rm=0&id=passive&ru=%2fApplicant%2fMyAccount%2fHome"><trust:Lifetime><wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2013-04-29T01:12:09.300Z</wsu:Created><wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2013-04-29T01:42:09.300Z</wsu:Expires></trust:Lifetime><wsp:AppliesTo
wctx	rm=0&id=passive&ru=%2fApplicant%2fMyAccount%2fHome

- Step 5: The relying party validates the Token with the public key provided by USAJOBS
  - The relying party extracts the Claims which includes:

    LastName, GivenName, Email, SessionID
  - The relying party then sets their session to authenticated

Within the SSO Token, the following Claims will be provided:

<AttributeStatement>

```
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/lastname">
        <AttributeValue>Jones</AttributeValue>
</Attribute>
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
        <AttributeValue>MyFirstName</AttributeValue>
</Attribute>
<Attribute
Name="http://schemas.microsoft.com/accesscontrolservice/2010/07/claims/identityprovider">
        <AttributeValue>login.usajobs.gov</AttributeValue>
</Attribute>
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
        <AttributeValue>MyFirstName.Jones@opm.gov</AttributeValue>
</Attribute>
<Attribute Name="http://schemas.usajobs.gov/identity/2013/04/claims/nameid">
        <AttributeValue>100000120</AttributeValue>
</Attribute>
<Attribute Name="http://schemas.usajobs.gov/identity/2013/04/claims/sessionid">
        <AttributeValue>292b6bcb-2e59-4b54-945c-f1112c9e96e4</AttributeValue>
</Attribute>
</AttributeStatement>
```

NOTE: Nameid is the Candidate ID.

Post Authentication Processing

Once the SSO Token has been received and validated, the vendor now has the option to request the account information if required. Depending on the integration between the TAS and the vendor, the account credentials may have already been passed. Because each TAS/Vendor relationship varies, the ability to request the User Account information is optional in the process flow. To support those vendors that need to establish or update an account, two new BODS were added to the SIF. **NOTE: Non TAS Vendors do not have access to other SIF related transactions outside of these two BODS.**

- BOD GetUserAccount. The GetUserAccount BOD allows the vendor to request the base account data used to establish or update a base account in their system. Using the SessionID returned with the Accepted SSO Authentication, the GetUserAccount will request this information from USAJOBS.

- BOD ShowUserAccount. Upon receipt of the GetUserAccount, the request will be validated by USAJOBS using the standard SIF Security processes. USAJOBS will return the ShowUserAccount with the status of the request and for Accepted transactions, the corresponding data for the job seeker account will be returned.

SSO Federated Metadata

All metadata associated with SSO is located on the schemas site. The following references have been added:

- SSO Token Example is located at:

  https://schemas.uat.usajobs.gov/Documentation/SSO/SSOToken.xml

- GetUserAccount BOD is located at:

  https://schemas.uat.usajobs.gov/Samples/GetUserAccount.xml

- ShowUserAccount BOD is located at:

  https://schemas.uat.usajobs.gov/Samples/ShowUserAccount.xml

- JAVA Example Code is located at:

  https://schemas.uat.usajobs.gov/Documentation/SSO/SSOJAVA.txt