Add a Transformation with Link to Certificate

The following steps outline the procedure for adding a Transformation with a link to the certificate:

1. Add the Transformation file for the following file to the Repository:
   TransformationsOfConfigFiles/OAuthServer/OAuthServer.Plugins.json
   For more information about setting up SSO, follow the steps in the Example: Setup of Aras Innovator SAML 2.0 Authentication with Azure as Identity Provider section.
2. Set the content to the Transformation file with links to secure files. An example follows:

```
{
 "@jdt.merge": {
   "@jdt.path":"$.['OAuthServer.Plugins']",
   "@jdt.value": [
      {
       "Name":"Aras.OAuth.Server.Plugins.Saml2Authentication",
        "Enabled": true,
        "Options": [
          {
           "AuthenticationType":"Saml2-AzureAD2",
           "DisplayName":"Saml2 Google with signing",
           "ServiceProviderOptions": {
      "EntityId":"https://{OAuthServerURL}/Saml2-AzureAD/"
            },
           "IdentityProviderOptions": {
             "EntityId":"https://accounts.google.com/o/saml2?idpid=C014h6zu2",
              "MetadataSource": "MetadataOptions",
              "Metadata": {
               "SingleSignOnService": {
                 "Location":"https://accounts.google.com/o/saml2/idp?idpid=C014h6zu2",
                  "Binding": "HttpRedirect"
               },
              "WantAuthnRequestsSigned":false,
               "SigningCertificate": {
                 "SourceType": "File",
                "FilePath":"/secure_files/stg-Google_2029-5-7-91113_SAML2_0.pem"
               }
             }
```


```
            }
          }
        ]
      },
      {
       "Name":"Aras.OAuth.Server.Plugins.GenericUserMapper",
        "Enabled": true,
        "Options": [
          {
           "AuthenticationType":"Saml2",
           "InnovatorUserNameFormat":"{uid}",
            "ClaimActions": [
              {
               // Validate uid (default Innovator users are denied).
                "ActionName": "Validate",
                "ActionOptions": {
                  "ClaimType": "uid",
                  "AllowPattern": ".+",
                 "DenyPattern":"^admin$|^root$|^vadmin$|^authadmin$|^esadmin$",
                  "PatternOptions": [ "IgnoreCase", "Singleline" ]
                }
              }
            ]
          }
        ]
      }
    ]
}
```


```
}
```

1. **Important**

   The secure files will be in the secure_files folder. Use the secure_files folder when configuring the FilePath.

For more information about full flow, refer to the Example: Setup of Aras Innovator SAML 2.0 Authentication with Azure as Identity Provider section.

For more information about configuring the SAML plugin, refer to the SAML2 Authentication Plugin Configuration section.

For more information about how to map users, refer to the Generic User Mapper section.