**Speeder IDP Integration**

**How As is Authentication works via LDAP**

* User launch application in browser.
* Network Authentication Pop up is displayed to enter user/pass, if no dedicated HTML login page is defined for App.
* Lego Struts Framework configuration is defined in strurts-config.xml file, where all action mapping and Form Beans are defined.
* It has Request processor configuration, which points to fwk-struts jar of LEGO. Each request is parsed through this Wrapper class around it to process user and related meta data
  + Init session
    - Create user Instance and hold it in http session
  + Process Auth Header
    - Performs below checks
    - If user isNotAuthenticated and isNotTimeout and isAuthHeaderPresent
      * Create AuthInfo Object that hold user credentials
      * Check isAuthHeaderCorrect
        + Extracts User info from header.
        + Throws FWK expection if no user info available in headers.
        + If isAuthHeaderCorrect -> Through SpdSecurity Manger authenticate user info

Security Manger internally calls LDAP directory and re authenticate user in backend.

If successful then init user which stored user id in SPD user object.

Set Profiles in user object coming from LDAP linked to log in user.

* + - * If all ok then Parent Request Processor do execute and lands user to landing page.
* How Profiles and Authorization is handled
  + Define fwk Custom Tag lib class known as fwktag.tld where all custom tags linked to a application are defined.
  + Process via tag class -> com.inetpsa.fwk.taglib.InitBlock which is used to check profiles defined in Jsp contains user profiles .
    - initBlock: Defines a set of HTML blocks displayable according to a condition on the current user's profile.
    - Block : Defines part of the HTML block to display depending on whether the condition is respected or not.
  + For example in jsp we define this init block
    - <fwk:initblock id="central" profiles="AdminCentral" operator="OR"/>
  + Then each request is routed through this tablib class which checks if profiles Admin Central is available in list of users profile
  + If it’s available then this block value is true and it’s executed at jsp level to show/hide html elements or navigation menus.

**Solution to remove LDAP Authentication and Create Custom Wrapper classes to process profile fetched from IDP JWT token**

* User launch application in browser
* User is now redirected to IDP Stellantis login page instead of custom App login page or network popup.
  + This url contains client id and the call back URL which user will land after successful login attempt.
* User enters his user/pass and below process executed in backend
  + Execute callback Action
  + From request parameter’s fetch authorization code
  + Call IDP access token API to get JWT token with below request
    - code
    - grant\_type
    - redirect\_uri
  + Get JWT token
  + Validate JWT token
  + Decode JWT token and fetch logged in users profiles and user info
  + Create custom Request processor and its Wrapper specific to Speeder application
    - Each request is passed through this processor same as in LEGO Framework
  + Modify struts\_config.xml to point to this custom Request processor
  + After info is parsed from JWT , perform below actions
    - Init session with use of Helper class ( fwk)
      * Create user Instance and hold it in http session
    - Process Auth Header
      * Performs below checks
      * If all validations are ok then init user which stored user id in SPD user object
      * Set Profiles in user object coming from IDP JWT token to logged in user.( SPD object)
        + Fetch all configuration of profiles available in fwk.xml
        + Iterate through this and check if current users profile is in above list , if Ok then

Create HashMap and store corresponding Matched Class Type as key and Profile name as Value in HashMap

* + - * Update SPD user object and set Profile with above HashMap
      * Rest flow is AS IS
      * Create custom Tag Lib Processor and modify fwktaglib.tld
        + <tagclass>com.inetpsa.spd.security.action.InitBlock</tagclass>
      * Now similar to LEGO process is same , but in this new behaviour we will check for SPD user object and not LDAP User object
      * Redirect User to expected landing page.