|  |
| --- |
| **Section A: Enrollment and Identity Proofing**  When onboarding a new user(s), how do we verify they are who they say they are |

First the user needs to sign up.

We verify if people are who they say they are with the following process:

1. Resolution
   1. The organization collects the name, address, date of birth, email, phone number, and employee ID number.
   2. The user can use a webcam to share their form of identification with their webcam.
2. Validation
   1. The system validates the user with two things:
      1. Their form of identification, such as a drivers license or passport
      2. Their signature
3. Verification
   1. The applicant is asked to take a picture of themselves.
   2. The applicant is asked to take a picture of their form of identification.
   3. The applicant is shown a pin code.
   4. The applicant is asked to go to a website from the web browser on their smartphone.
   5. The applicant is asked to enter in the pin code shown on their computer on the website on their smartphone.
   6. The applicant is asked to sign the touch screen displayed on their smartphone.
   7. The system then authenticates the signature, identification, and photo.
   8. If the system can successfully authenticate the user, the user is then registered,

|  |
| --- |
| **Section B: Authentication and LifeCycle Management** How do users authenticate to a specified system? (UserName/Password, SSO [Kerberos, SAML ...], ) Password rotation policy. |

Once signed up, the user in question needs to sign in. Users will be required to use multi-factor authentication:

1. Multifactor authentication is done with the user’s smartphone. The following MFA apps are acceptable:
   1. Two factor authentication
   2. Google Authenticator
   3. Microsoft Authenticator
   4. Authy
   5. Duo Mobile
   6. 2FA Authenticator (2FAS)
   7. LastPass Authenticator
   8. Salesforce Authenticator
   9. LastPass

|  |
| --- |
| **Section C: Federation and Assertion** Password Reset |

1. This is how users reset their password if they forget.
   1. The user clicks the forget password link.
   2. The user enters in the email that they signed up with.
   3. The user clicks the clink that is sent to them in their email.
   4. The user enters in a new password.
   5. The user clicks submit.