Credential Management Specification/Use Cases/Example

Initial Draft 20160519, WCurry, Review and comment to improve, etc.

Intended to accompany the TIER IAM BackBone Scenario .

Credential Management: Use Cases, Specification and Rule Examples

A set a features that are fairly common in nature across institutions are shown in a table below. Following the table are possible kinds of logic that might need to be involved in the features.

It is likely that the details of those logic bit would be the primary difference from implementation to implementation. It was discussed recently August 2018 that perhaps driving much of this logic with groups and code components referencing the groups could isolate many of the differences into institutionally managed code for group memberships. Thus the Account UI could be developed in a more general manner for multiple institutions to leverage. CSP schools have expressed interest in building this feature out. Question from working group is should this be a part of the TIER deliverable.

Table of event/features to include:

Account Create	**Self service account create/claiming, allow for invite, claim at website or similar UI feature with SMS or email codes provided to previously known user email or phone.**	
Account Credential Change	Passwords and Two factor self service. Each can be self service or assisted by helpdesk. Helpdesk staff cannot know or have control of the credential being changed they can only send user an event prompt/secret for use in the self service interface.	
Account Credential reset (forgot, etc)	Password and two factor issues. The user is not in control or does not know the values of the credential (password), This is a bit harder case often forgot password , or issue with multi factor.	
Account Disable /Enable	Admin Account management panel - this is done by admin users in response to an issue with the user or the account.	
Account Expire /Unexpire	Automated Deactivate and activate account based on the membership in the groups defining eligibility for account(s).	
Password Expire	Timed expiration of a password.	

- **Account Create:**
    - **Administrative Add Process**
        - Administrator uses form on "new user" screen of Admin UI to fill in basic user data including user name and initial password
        - Administrator sends email to new user including acceptance page URL, username and (one-time) password
        - New User browses to acceptance page, enters username and one-time password
        - New User enters and confirms new password when prompted
        - New User Enrolls in MFA
            - install/configure app on phone, tablet, etc
    - **Invitation Process**
        - When person data store attains qualifying person data
            - (rule example: affiliation qualified, Name provided, dob, personal email, one or more of the following phones(work office, work mobile, home, home mobile) trigger:

      Send Invite to personal email and/or SMS

            - one time use security code
            - expire in _nnnn_ minutes (configure duration)
            - record if security code used

Invitation Response Create Process

- User goes to UI webpage

- Enter one time use security code
- Correct security code and was it entered within limit?
- User successful:
    - prompted for Enterprise UID,
    - prompted for DOB,
    - selects known last 4 digits from list of 6 masked phones
    - User is presented with account names available
    - User selects one of the available names
    - Record and bind user name to person
- When code not used within time limit:
    - Administrative Console can Re-Invite Helpdesk
        - Send new invite
        - User performs Invite process above
- Establish Credential (password)
- Account Information Management
- Provision Account to Authentication Store(s)
- Confirm Provisioning with User Email Communication

Account Credential Change: (user must know current value)

- Self Service Change Process
    - User authenticates to Credential Change Service
        - username/password
        - MFA
    - User Enters new Password
    - Establish Credential (password)
- Account Information Management data saved
- Provision Account to Authentication Store(s)
- Confirm Change with User Email Communication

Account Credential Reset: (user does not know current value)

Self Service Reset Process

- User responds to Dialog to confirm their identity
- User receive the verification code
    - User provides enters code
    - max 3(n) tries block further attempts for lock period
    - send message to user email

Establish Credential (password)

- Account Information Management data saved
- Provision Account to Authentication Store(s)
- Confirm Change with User Email Communication

Helpdesk Assisted Reset Process

- User Call / Opens Ticket with Helpdesk
- Helpdesk User Confirms User Identity
    - User receive the verification code
    - User provides enters code
    - max 3(n) tries block further attempts for lock period
    - send message to user email

Establish Credential (password)

- Account Information Management data saved
- Provision Account to Authentication Store(s)
- Confirm Change with User Email Communication
- **Password Composition Rule:**
    - (Note: Password composition Rules can vary for an individual account based on attributes about the account, in this example we call this Password Level. An implementation can support 1 to N password levels. The level is a reflection that controls and allows policy to be implemented based on access granted to the account. An access permission granted to an account would set a value on the registry entry that binds the account to the user entity. The levels control password parameters such as minimum password length, composition, days before expiration. The attributes may change over time based on access permitted to the account and can cause the need to change a password due to such a change. Example could be the account has an access to allow PCI access and thus must expire every 90 days. This change would trigger the need to alter password if the current password duration expires in > than 90 days. Let's say access is set in a manner of 5 levels.
    - Self service
    - Updates/view sensitive data for a department/college
    - Updates/view sensitive data for institution wide basis
    - Updates/configure an application, server/vm, middleware, network, PCI/FBI, standards.
    - FISMA Moderate controlled compliance
        - When: Invoked whenever collecting new value for password:
        - Acceptable Characters set –

        - (example: A-Z, a-z, 0-9, special(.,!#$%^&*()<>?/;:)
        - Dictionary Check (must be at least 50K words/patterns)
        - Length of Password based on LevelofStrength = min x character
        - Duration of Password based on LevelofStrength = n days
        - Or
        - If Passphrase of at least 18 characters.
        - Some patterns will need to be checked like (111111111111111111111111111111111111111 not allowed)
        - Uses Acceptable Character set
    - **Two Factor Authentication Rule:**
        - EduPerson Faculty, Staff or Employee with info that included that includes them in the "Bronze level Access Group" may opt in to the TWO factor using self service**.**
        - EduPerson Faculty, Staff or Employee with Jobs that access PII or have Campus Wide access to Administrative Applications with restricted data will be in the group "Must have two factor auth" driven by the assigned access privileges.
        - If a person has been phished and do not use the Two Factor Auth services, then the individual will be added to the "Once phished then two factor" group.
        - All individual above will use the self service sign up for two factor service.
        - Weekly reports of individuals who should have two factor but have not enrolled will be produced and the Unit/college security administrators notified of the omissions.

Manage Account Profile

- Let user remove middle name from DisplayName attribute
- Let user upload a photo
    - Need an administrative console feature to approve photo
- Enroll existing users in MFA
- update contact information, personal email and SMS

Account Credential Disable/Enable:

- Action entry to disable/enable account
- Account Information Management data disable/enable
- Provision Disable/Enable to Authentication Store(s)
- Notify user via email to personal email (out of band)

Account Credential Expire/UnExpire:

Action entry to Expire/UnExpire account

- Account Information Management data expire/unexpire
- Provision expire/unexpire to Authentication Store(s)
- Notify user via email to personal email (out of band)

Password Expire:

When: current date time > password expire date time minus n days

- Send Warning emails to user to indicate password expiration is approaching. (email 1 per day for 7days prior to expiration)

- When: current date time > password expire date time or

Password level needs less days and/or more complexity

- Account Information Management data expired password set.
- Send password expire message to Authentication store at When condition above.
- Notify User by out of band email that institutional password just expired.