White Paper on Account Management

|  |  |
| --- | --- |
| Topic |  |
| What is Account Management | The ability for a person or business to define and manage who they and what they can do within a given solution. |
| Typical capabilities that the customer can establish for its account | Profile (address, alternate contact info, contact preferences)  Multiple user access, and permissions for each user |
| Verifying that the account is for a legitimate user | Email confirmation of account activation is sent to the registered email. The email address is used as a unique identifier, helping to ensure that it’s a unique communication. Captchas are also used to remove any “bot” account creation |
| Difference between account management for customers and for the agency’s own employees | Business Process:  Individual business practices around security, accessibility and workload distribution will be different than the needs of external customer account access.  Security: internally, access to systems can be maintained within a firewalled domain. Customer access to certain systems requires external domain access, which requires more attention paid to the specific systems you are allowing access to.  Usability - external customer account management is designed as a self-service mechanism. Internally, account access is usually centralized through an organization’s IT system administration department. |
| Why customer account management is not performed in the agency’s own Active Directory | Security: keeping external domain entities out of your Active Directory means there is no reason to expose AD externally, which improves security.  Supportability: managing an indefinitely growing and changing public population of accounts is impractical  Usability: a separate claims-based authentication framework for your customers gives you greater control to define a process that is efficient and tailors to the nature of the your customer base |
| Relationship to Electronic Signature | The unique content captured in the profile can be used as an electronic signature. A combination of email, birthdate, and sign date, for example can be a valid electronic signature given that those attributes provide a unique “key” for a given account. |
| Techniques to authenticate the customer |  |
| Industry best practices |  |
| Workload on the Help Desk | Key self-service features can drastically reduce workload   * Automated password reset * Automated username retrieve * Account consolidation * Built in FAQs and chat |
| Impact on business process – Duration |  |
| Completeness |  |
| Notifications | * Email notification, particularly when email is the unique identifier is an efficient communication mechanism that provides targeted communications * Other notifications for marketing, outreach, etc. should have an opt-in opt-out feature on the profile * Typical automated notifications include:   + Welcome email   + Registration confirmation   + Submission confirmation   + Password reset confirmation   + User Account addition   + User account changes notification |
|  |  |
|  |  |
| Value to the Customer |  |
| --Guidance in submittal | This is more general self service portal - not really account management |
| --Submit increments | This is more general self service portal - not really account management |
| --real-time feedback on mistakes or missing information | This is more general self service portal - not really account management |
| --single account for all interactions with the agency | By being uniquely identified to the organization, the user experience is improved by   * Single data entry, multiple application * Account history across functions * Payment history across functions |
|  |  |
|  |  |
|  |  |
| Value to Business Partners | Business Partners are like customers. They will have |
| Value to the Agency | Account Management is the key to Constituent Management. Being able to define your customers (who they are, what they do, how they do it) is the first step to providing a digital engagement platform that is designed to support your constituents. |
| Capability Maturity Model |  |
| Level One – Online access to download forms | Publically accessible site that allows anyone to download a copy of the form. No account management is required, but a standard practice is to capture contact information as a condition of providing the download link. This allows for tracking of potential customers. |
| Level Two – Complete an electronic form online such as Adobe | Publically accessible site that allows anyone to fill out a copy of the form. No account management is required, but a standard practice is to capture contact information as form attributes: Name, Address, phone, email. Note that the submittal must have a unique identifier assigned to it during submission (transparent to the submitter). |
| Level Three – Create account for single submittal | Data model includes:  Account Holder- ID, name, company, address, email, phone  Enhancements: preferred means of notification (eg: email, phone, snail mail) |
| Level Four – Account for multiple participants and applications | Data model includes:  Organization (ideally using the same organization entity as is used by the corporate database)  Individual  Role  Role for the individual  Enhancement: Role for the individual specific to the company. This is important for consultants that may help multiple companies with their applications where for one company the consultant has a different role than for another company.  Note: making the individual’s role different for each program is addressed in Level Five of the account management capability maturity model. |
| Level Five – Account used across agency programs | This level requires that programs SHARE a single account management data model. Ideally the software used by each program would also share (ie Consume) the same account management module.  Data model includes |
| Level Six – Agency-wide account management |  |
| How account management used in Dept of Business Oversight | Businesses can establish an account online and then apply for or renew their licensure. All required documentation can be submitted online as part of the application process. A business can submit some documents via traditional snail mail if desired by including the application ID assigned through the portions of the application submitted online. Snail mail documentation is scanned and then linked to the application submitted online.  An individual exists in the DBO database online one time. All businesses associated with that individual are then linked |
| Agency data management to enable higher levels of account management | Applications across the agency must cooperate to implement account management for customers and business partners.  Some might advocate putting external customers into the agency’s Active Directory or other LDAP service. It is possible to design for a federated LDAP that puts one Active Directory outside the protected zone for customers and another Active Directory inside for employees.  This topic is addressed in a technical appendix.  The account management service must provide a sufficiently broad range of data relationships that anticipate what individual business areas will require to meet their program and legal requirements.  Hesitation to allow online accounts that serve as an electronic signature is rarely if ever based on a legal restriction. Federal and State laws make electronic signatures possible for virtually every government program. There is a difference between an inability to accept the opportunity for change and an actual legal impediment to change.  Key data model relationships to define “up front” include:  Individual  Organization (Applicant)  Individual to Organization  Role  Program  Organization to Program  Individual to Organization to role to Program (should order of role and program be changed?)  Program representatives should agree on a shared set of Roles allowed in the preparation and tracking of an application.  Customer organizations may participate in multiple programs from your agency. It is not practical to expect an organization to have centralized control over its divisions that may do business with your agency. What the agency will benefit from with a central account management function is the ability to link all the divisions of a customer organization together to a single organization name. Among other benefits, this enables the agency to know the extent to which a single organization interacts with the agency.  Each customer organization division can have its own account manager, its own address, and other contact information. (NOTE: is this true? Are organization division addresses based on the individual?) |
| Governance issues in account management | Strong Password Guidelines – standard practice is to create strong password rules, and then require that passwords are periodically updates. This can create usability issues if your customer base logs in infrequently  Account Retention – define a policy for removal of closed accounts. Typically 6 months to 1 year is a standard practice |
| Managing a single instance of the account management service to support multiple business programs. |  |
| Managing a data model that is shared across multiple agency program areas. | The Organization entity and the Individual entity are two prime candidates where the account management service uses data entities already established by the Agency as part of an enterprise-wide (integrated) database. The Department of Business Oversight has one entity for Organization that is used across the enterprise by all licensing programs. This Organization entity is also used when an individual is creating an account on behalf of an organization for purposes of submitting license applications and other business functions online. |