# Requirements Overview

This document defines the functionality needed to successfully implement Active Directory and user access to the Philly311 CRM solution on Salesforce.

# Workshop Attendees:

* Tom Gagne
* Shane Ace

# Requirements

#### Microsoft Active Directory Federated Services (Single Sign-On)

The City manages end user authentication using Microsoft Active Directory. The use cases for utilizing the Microsoft Active Directory Federated Services integration are:

1. Manage End User Authentication using the City’s Microsoft Active Directory.
2. Manage SFDC End Users using the City’s Microsoft Active Directory
3. Enable End Users single sign on to the SFDC platform

# Action Items – The City

The City of Philadelphia will provide a Microsoft Active Directory Federated Services version 2.0 prior to developing the Microsoft Active Directory Federated Services integration.

# Action Items – Unisys

Unisys will resolve significant Deviations from the Design Document that arise from the testing for those Service Requests and Interfaces that are designated as the responsibility of the Unisys staff. This will consist of:

* + Validation of the Active Directory use cases for SFDC End Users.

Philadelphia requires configuration or development of interfaces to support multiple constituent facing channels: For Implementation, Unisys will:

* Configure Single Sign-On using Microsoft Active Directory Federated Services

Unisys will conduct the following activities for the channels and platform integrations described previously in this section.

* Develop, distribute and review Integration Design Document (enhanced from the previous version developed for the Pilot solution with the following topics)
  + MS Active Directory Integration Design Document
* Develop and unit test each channel configuration and integration
  + MS Active Directory Integration

Unisys will resolve significant Deviations from the Design Document that arise from the testing for those Service Requests and Interfaces that are designated as the responsibility of the Unisys staff. This will consist of:

* + Validation of the Active Directory use cases for SFDC End Users.

# Deliverables

* Technical Requirements Definition Document
  + MS Active Directory Integration Requirements Definition Document
* Technical Detail Design Document
  + MS Active Directory Integration Design Document
* Configured/Developed the channels and integrations
  + MS Active Directory Integration

# Assumptions

The Unisys Team assumes that the City manages end user authentication using Microsoft Active Directory.

# SOW Appendix C Requirements

| **Reference Number** | **Service Request Requirements** | **Type** | **Implementation Plan** | **How Provided** | **Workshop Notes** |
| --- | --- | --- | --- | --- | --- |
| 2.06 | The solution provides the ability for a constituent to use a single account log-in to access a variety of City services regardless of the department offering the service for the purpose of submitting or tracking requests | F | SFDC Service Cloud application will be configured for Single Sign-on authenticating the users against City's Active Directory using SAML. | SFDC Service Cloud | Users inside the City’s network authenticated using MS Active Directory will only be allowed to login using single sign-on. |
| 3.12 | The solution provides ability to manage different permissions for access to data and service request types based on user profile | F | SFDC Service Cloud application will be configured to implement this requirement | SFDC Service Cloud | Permissions are administered using profiles. Users will be assigned a profile in SFDC. |
| 7.10 | The solution provides the ability to be accessed from a mobile device (smart phone, tablet, etc.) | F | SFDC Service Cloud application will be configured to work in most recent mobile browsers like Apple Safari for iOS and Google Chrome for Android, however it is recommended to use SFDC on a smartphone in a native app due to limitations in rendering engines on mobile browsers. | SFDC Service Cloud | Single sign-on will only be supported by accessing SFDC using a City networked computer. |
| 12.02 | The solution provides tools for managing user accounts, security settings on data and/or applications | F | The SFDC Service Cloud application will be configured to implement this requirement - all users and application level security will be defined and maintained by the City organization administrator, and not be provided by the salesforce.com support services. | SFDC Service Cloud |  |
| 12.03 | The solution utilizes active directory structure for assigning privileges and rights | CU | SFDC Service Cloud application will be configured for Single Sign-on authenticating the users against City's Active Directory using SAML. | SFDC Service Cloud | SFDC tools assigns a profile to a user account to enable privileges and rights. |
| 12.04 | The solution provides a flexible and secure security management process for assigning privileges and rights | F | SFDC Service Cloud application will be configured to implement this requirement. The application provides a flexible, layered security framework that to share different data sets to different users. Application administrators will have to create profiles, roles, hierarchies and rules that are enforced in the user interface, reports, dashboards, search results and the API. | SFDC Service Cloud |  |
| 12.05 | The solution provides the ability to grant authorization for access at the function level (e.g., manager, department head/director) | F | SFDC Service Cloud application will be configured by creating a sharing model to data and functionality. Additional workflow rules will be created to grant authorization for access | SFDC Service Cloud | Through a user profile. |
| 12.06 | The solution provides active directory integration to support single user sign-on | CU | SFDC Service Cloud application will be configured for Single Sign-on authenticating the users against City's Active Directory using SAML. | SFDC Service Cloud |  |
| 12.07 | The solution provides the ability to have technical controls for password timeout, complexity and reuse and length | F | SFDC Service Cloud application will be configured to implement this requirement.  Will work with the City administrator to configure the password requirements noted below: - Password expiration can be set for 30, 60, 90, 180 days, 1 year, or Never  - Password history may be set to anywhere from 1 to 15 passwords remembered, or none  - Minimum password length may be set to 5, 8 or 10 characters  - Password complexity can restrict the user to a mix of alpha and numeric characters, or alpha, numeric and special characters - User account lock may be set to 3, 5, or 10 attempts before lockout (This feature may be disabled as well if you wish no lockout)  - Lockout effective period may be set to 15, 30, 60 minutes or Forever (administrator must reset password)  - Sessions may be configured to timeout after 15 minutes up to 8 hours of inactivity, at which time the user is automatically logged out. | SFDC Service Cloud |  |
| 12.08 | The solution provides the ability to encrypt user IDs and passwords | F | SFDC Service Cloud application will be configured to implement this requirement by encrypting passwords vai the SHA algorithm with a 256-bit hash. This is a one way hash. User IDs are not encrypted. | SFDC Service Cloud |  |
| 12.09 | The solution prevents display or printing of passwords | F | Passwords are obscured during logon. SFDC Service Cloud application will be configured to not display or print passwords | SFDC Service Cloud |  |
| 12.10 | The solution provides the ability to delegate administration for user provisioning | F | SFDC Service Cloud application will be configured to implement this requirement. Salesforce.com supports a delegated or decentralized administration model, to better allow City to manage an environment that includes multiple administrators for different groups, business lines, divisions, etc. as required. | SFDC Service Cloud |  |
| 12.11 | The solution provides the ability for an administrator to suspend an ID from future usage | F | SFDC Service Cloud application will be configured to implement this requirement. Each user within an Org will be assigned a unique usernames and usernames cannot be duplicated. | SFDC Service Cloud |  |
| 12.35 | The solution provides an audit trail of all system activity, including by user, date and time | F | SFDC Service Cloud application will be configured for the following auditing features:  Record Modification Fields All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.  Login History You can review a list of successful and failed login attempts to your organization for the past six months.   Field History Tracking You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.   Setup Audit Trail Administrators can also view a Setup Audit Trail, which logs when modifications are made to your organization's configuration. | SFDC Service Cloud |  |
| 12.36 | The solution provides alerts for unauthorized or suspicious activity | F | SFDC Saas offering provides this capability , SFDC's operations team continuously monitors the system for unauthorized or suspicious activity. | SFDC Service Cloud |  |
| 12.37 | The solution maintains information on security events and can provide reporting on demand | F | As a part of the SFDC Service Cloud SaaS offering - The Operations Service Center (OSC) monitors the Production network 24x7 and is on call for issue resolution. Any potential issues identified by the monitoring tools provide visual and/or email alerts to OSC and other appropriate TechOps personnel. Alerts trigger analysis and response procedures. Further notification using established procedures may be executed based on the severity of the issue. In the event of an operational issue, Salesforce.com's goal is to rapidly restore service. The City may request these reports through the standard post production support processes described in the SOW. | SFDC Service Cloud |  |
| 12.38 | The solution provides summarized and detailed reports on user access, usage and audit logs, etc. | F | SFDC Service Cloud application will be configured such that the creator and last updater, as well as timestamps, are recorded for every record. All logins, both successful and unsuccessful, will be recorded for retrieval by the City's SFDC Service Cloud administrator.  Limited forensic evidence, if needed, is available from the web or application logs and can be provided for an additional cost by requesting it through the post production support desk. | SFDC Service Cloud |  |
| 12.39 | The solution allows the placement of a user-defined warning banner when logging into the application for all types of users (internal, web self-service, mobile self-service and mobile field worker) with ability to push different content to different types of users | F | SFDC Service Cloud application will be configured to implement this requirement. | SFDC Service Cloud |  |