



WEBSITE REDESIGN PROJECT
WINDOWS INTEGRATED AUTHENTICATION
(SSO VIA TIF) AND MISCELLANEOUS INTRANET
SERVICES

CHANGE ORDER

Prepared by:



1572 E. Capitol Drive
Shorewood, WI 53211

Tom Pappas

Business Development

Phone Number: 414-914-9143

Support Line: 414-914-9300

July 6, 2017

CONTENTS

OVERVIEW	3
APPROACH	3
TASKS	7
ASSUMPTIONS	7
DURATION	8
TOTAL HOURS / PRICE	8
TERMS.....	8
APPROVAL.....	8

OVERVIEW

The County has requested the ability to use Windows Integrated Authentication with sites hosted in their Titan CMS instance, specifically the County Intranet.

After reviewing options with the County team and gaining an understanding of the future hosting environment for the Titan CMS instance, it has been determined the preferred solution is to implement the Titan Identity Federation (TIF) module to support the County's need for Windows Integrated Authentication.

This Project Enhancement Request covers the effort required to implement the Titan Identity Federation for the County Titan CMS instance within the future hosting environment for the County's Titan CMS instance.

The goal of this enhancement is to provide County Staff seamless access to the Milwaukee County Intranet and other secured content hosted in the County's Titan CMS instance when they are accessing the content from a workstation connected to the County network and authenticated with a valid County domain user account.

The County Titan CMS instance is currently using Titan's External Authentication Module to allow for Active Directory Integration. This module is designed to use Forms Authentication to authenticate against a local or remote Active Directory domain. The County would like to continue authenticating against the same Active Directory domain, but add the ability to authenticate with Windows Integrated Authentication for users connected to the County internal network, authenticated against the domain, and using a current browser supporting Kerberos and NTLM. Support for authenticating users via Forms Authentication when they do not meet the criteria for Windows Integrated Authentication is required.

In addition, Milwaukee City also uses the Titan External Authentication Module to authenticate against their internal domain. In the current hosting environment, the External Authentication Module has the ability to access both the County and City Active Directories.

With the hosting environment being moved to a new physical location, support for Active Directory authentication must be maintained for both the City and County.

APPROACH

In order to support the requirements for this enhancement, Northwoods will leverage the Titan Identity Federation (TIF) Module. The module supports Windows Integrated Authentication. Combining this module with the existing Titan External Authentication module, the requirement to support Windows Integrated Authentication with Forms Authentication as a backup is met.

In addition, if the City of Milwaukee chooses to remain with their Forms Based Titan External Authentication module, they will be required to setup a site to site VPN with the new County environment or permit LDAPS traffic from the new County hosting environment's public IP address to one of their Active Directory domain

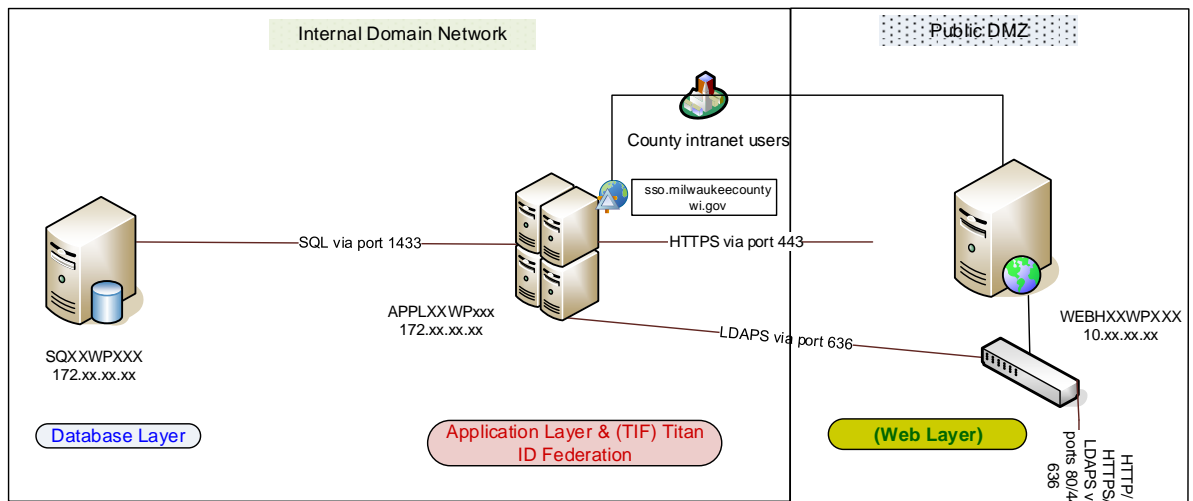
controller. If either option is a concern for the City, the TIF module can be setup to allow them to direct their users to a TIF authentication server hosted in their environment without the need to setup a VPN or open the firewall to the new County environment.

The TIF & External Authentication module joint solution consists of the following elements:

- Single Sign-on Block hosted in the Titan CMS instance configured per Content Site
- Titan Identity Federation Authentication Server hosted on a member server for the Active Directory domain being authenticated against
- Titan External Authentication Module (hosted on the Titan CMS instance and/or TIF Authentication Server). NOTE: City/County has customized External Authentication Module supporting server-less binding and LDAPS protocol. Solution assumes these features will be carried forward.

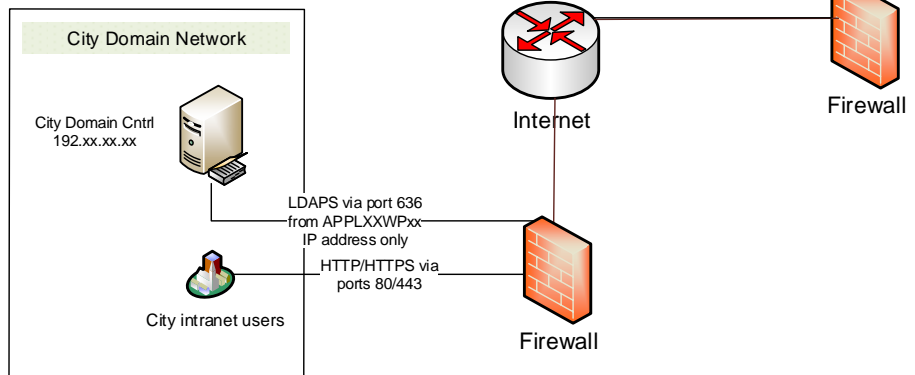
The following diagram illustrates the infrastructure for the solution assuming the City does not implement TIF:

Milwaukee.Gov Version 6.X
Production System Architecture Design



NOTES

- This solution allows the county to use windows authentication by way of the Titan Identification Federation (TIF) module to achieve a SSO type of functionality.
- This solution also allows the city access to their intranet by way of port 636 LDAPS using static IP's
- With this solution the city will also be able to access everything from the new data center in MAD/EDP Oneneck

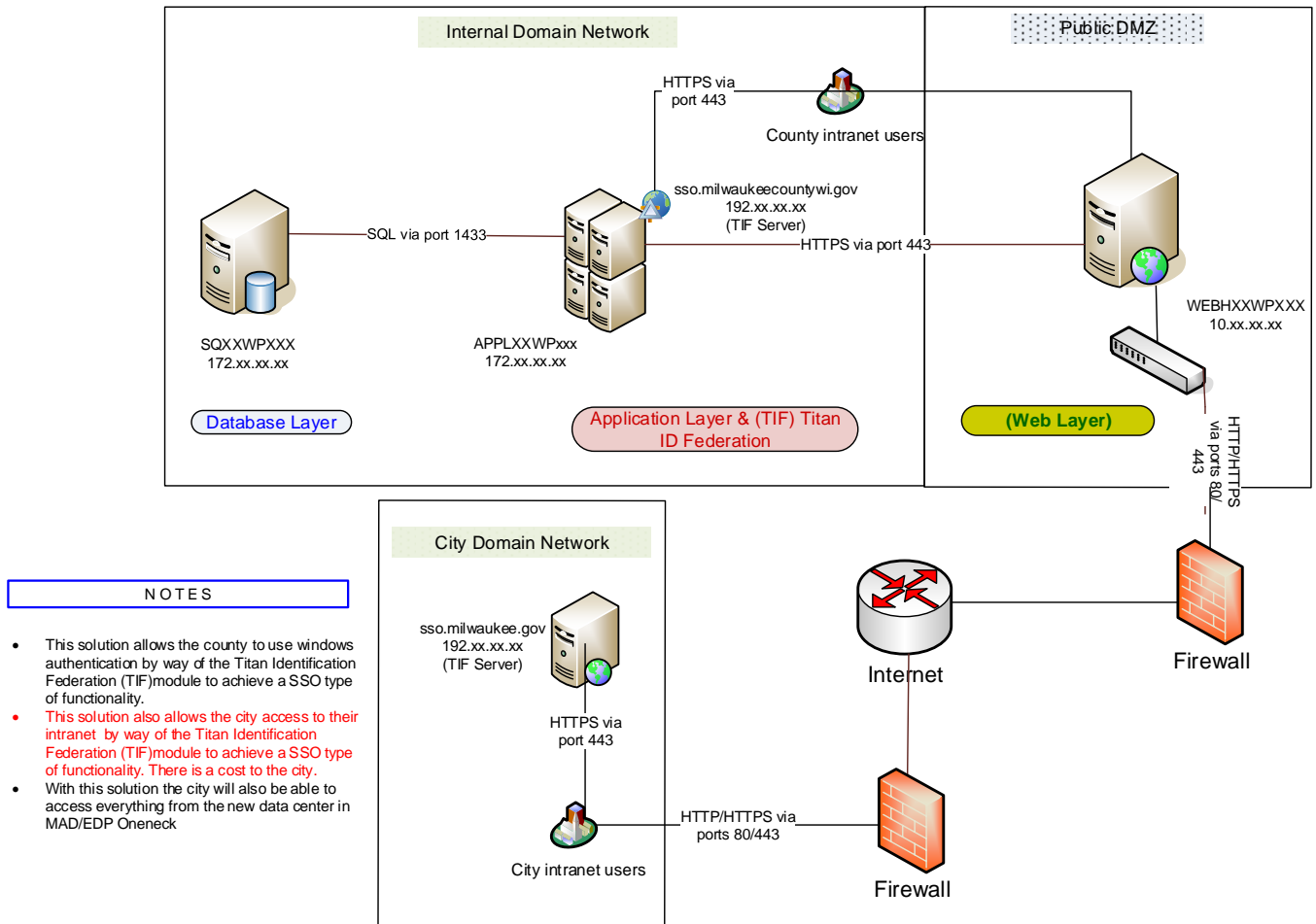


The solution requires each Content Site have a default login page defined. The page hosts the Single Sign-On Block which is designed to work as follows:

1. Checks if user is already authenticated.
2. If so, checks if user was redirected due to permission failure or is coming to the page directly.
 - a. If redirected due to permission failure, the block informs the user they do not have access to the requested resource.
 - b. If user is coming to page directly, the block renders a welcome message for the user and provides a link to log out.
3. If user not authenticated, a client-side check is made against the Titan Identity Federation Authentication Server domain to determine if the client has access to the domain.
 - a. If client cannot access the domain, a web form is provided to allow login via the Titan External Authentication module.
 - b. If client can access domain, the user is redirected to the TIF Authentication Server for authentication.
4. The TIF Authentication User attempts to retrieve Kerberos ticket to perform Windows Integrated Authentication for the user.
 - a. If user is authenticated with Windows Integrated Authentication (WIA), a secure token is created with public/private key encryption and the user is redirected to the Titan Login page they were referred from with the token.
 - b. If the user is not authenticated via WIA due to inability to retrieve token (i.e. unsupported browser) or invalid token, the user is presented with a web form allowing login via Titan External Authentication Module. On successful login, a secure token is created with public/private key encryption and the user is redirected to the Titan Login page they were referred from with the token.
5. On return to the Titan Login page, the secure token is decrypted using public/private key decryption.
6. If Titan fails to decrypt and valid the token, the user is presented a message indicating login failure and provided a link to re-attempt their login.
7. If Titan successfully decrypts and validates the token, the information contained in the token is used to authenticate the user against Titan's local user store. The authentication process creates the user in Titan if they do not exist, then assigns groups defined within the security token to the user, removing any from previous authentications that the user no longer belongs.
8. Once the user is authenticated, they are directed to the page they originally requested.

The following diagram illustrates the infrastructure required if the City does implement TIF:

Milwaukee.Gov Version 6.X
Production System Architecture Design



Whether the City of Milwaukee implements TIF or establishes the appropriate connectivity to the new Milwaukee County environment to support their existing solution, the solution will provide Milwaukee County seamless Windows Integrated Authentication for their internal users with Forms Authentication backup for their external users.

TASKS

NWS will perform tasks:

- Integrate the core TIF module into the Milwaukee County Titan CMS master solution (14)
- Update the Titan External Authentication Module developed for the Milwaukee County Titan instance with modifications required to support TIF, integrate module with core TIF module (12)
- Install and Configure the TIF Authentication Server in the new Milwaukee County hosting environment (4)
- Styling, setup and configuration of the Titan Single Sign-On block for the County websites (4)
- Quality Assurance (8)
- Deployments, Project Management (8)
- Professional services pertaining to the Intranet (92)

Hours: 142 @ \$140 / hr Total \$19,880

NWS Team: Senior Tech Lead, Senior Developer, Account Director

ASSUMPTIONS

- Northwoods is providing the project at a reduced hourly rate of \$140/hr from \$155/hr. The price reduction is limited to this PER.
- Server-less binding and LDAPS features implemented for the City and County previously need to be maintained. Core TIF module will be modified as necessary to maintain support for these features.
- County's TIF Authentication Server will reside on a server that is a member server of the Milwaukee County domain end users are authenticating against.
- County is self-hosting Titan CMS and the TIF Authentication Server, thus, the County is responsible for ensuring end users can reach server resources as appropriate given requirements from Northwoods.
- The City of Milwaukee will continue to share the County's Titan CMS instance. The bulk of cost involved with implementing TIF is tied to setup and configuration as well as integration with the existing City/County External Authentication module. As a result the cost to the City of Milwaukee is limited to setup and configuration of their TIF Authentication Server and effort for configuring and styling the Single Sign-On block for their websites. Here is a breakdown of the costs to the City of Milwaukee should they choose to implement TIF to gain Windows Integrated Authentication support:
 - Install / Configure TIF Authentication Server in the City of Milwaukee hosting environment (4 hrs)
 - Style, setup and configure the Titan Single Sign-On block for the City websites (4 hrs)
 - Quality Assurance (2 hrs)
 - Deployment services and project management (4 hrs)

NOTE: If TIF is implemented for the City sites as part of this PER, the 14 hours estimated above will be at the reduced rate of \$140/hr.

DURATION

- Once approved we expect the Tasks to take 2 to 4 weeks to complete.

TOTAL HOURS / PRICE

142 hours @ \$140/hr \$19,880 (County only TIF implementation and miscellaneous services)

64 hours @ \$140/hr \$8,960 (If City TIF implementation is included in the PER scope)

Please Select Approach

TERMS

- 100% of selected Approach due upon Task completion and acceptance by the County. County will make best efforts to review Task completion and give its feedback or acceptance within two (2) weeks.

APPROVAL

Date: _____

Milwaukee County

Signed: _____

Printed Name: _____

Title: _____

Northwoods Software Development, Inc.

Signed: *Patrick Bieser*

Printed Name: Patrick Bieser

Title: President