CTS Advisory Council

Office 365
Tenant Design

July 2014
What We Said
Opportunity

• Microsoft is presenting a licensing option that offers attractive pricing for subscription-based licensing in the Cloud even if you don’t use Office 365 cloud-based applications

• Once deployed, these licenses must be activated in the Cloud and re-activated every 30 days

• Managing license activation can be labor intensive without the use of:
  – A sync engine (DirSync or FIM) to automate creation and maintenance of tenant accounts
  – An authentication engine (ADFS) to eliminate need to re-enter credentials for license authentication
CTS Response

To meet customer needs for O365 license activation, CTS will provision:

- A single shared tenant
- A process for managing the shared pool of licenses
- A single synchronization engine using Forefront Identity Manager (FIM)
- A single authentication connection using Active Directory Federation Services (ADFS)
## Alternatives Considered

<table>
<thead>
<tr>
<th>Multiple Cloud Tenants Distributed License Administration</th>
<th>Shared Cloud Tenant Central License Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Customers provision separate O365 tenants, manually import EAD data, manually administer licenses</td>
<td><strong>3</strong> CTS provisions a shared Statewide tenant with one DirSync and one ADFS connector</td>
</tr>
<tr>
<td>CTS provisions multiple ADFS connections, one for each tenant</td>
<td></td>
</tr>
<tr>
<td><strong>2</strong> Customers provision separate O365 tenants</td>
<td><strong>4</strong> CTS provisions a shared Statewide tenant with Forefront Identity Manager (FIM) and one ADFS connector</td>
</tr>
<tr>
<td>CTS provisions multiple DirSync connections and multiple ADFS connections, one for each tenant</td>
<td></td>
</tr>
</tbody>
</table>
Multiple vs Shared Tenant

• Multiple tenants, one per agency
  – Higher operational maintenance cost
    • Multiple DirSync/FIM and ADFS connections, one per tenant
    • Must be undone if state moves to O365 services
  – Agency manages their own licenses
• Shared tenant
  – Lower operational maintenance cost
    • One DirSync/FIM and ADFS connection
  – CTS manages a shared license pool
    • Creates a need to establish license management processes
DirSync vs FIM

• Both products
  – Require enterprise administration rights to install and manage (and thus CTS involvement)
  – Require review and remediation of EAD attributes needed for synchronization

• DirSync
  – Is “free” and will require some infrastructure to implement
  – Does not filter content (syncs all 190 EAD attributes)

• FIM
  – Is a purchased product and will require more infrastructure to implement
  – FIM filters content (5 required EAD attributes)
CTS Direction

If customers pursue the purchasing of O365 licenses, CTS will provision:

- A single shared tenant
- A single synchronization engine - FIM
- A single authentication connection – ADFS
- A process for managing the shared pool of licenses
Update
Challenges

• Agencies who have purchased O365 licenses are keenly interested in using the SharePoint service
• Use of a single, shared tenant means CTS would have to be responsible for all O365 SharePoint administration including creating and maintaining site collections and managing storage
• Research into options for managing a shared license pool has not reveal promising solutions
• Microsoft cloud Identity Management services are evolving as we work on this project
O365 Multi-Tenant Design
How This Will Work

• CTS will manage one instance in Azure Active Directory (AAD) for the state (wa.gov)
• CTS will manage one connection between Enterprise Active Directory (EAD) and AAD to provide directory synchronization (FIM) and authentication (ADFS)
• Each agency will work with Microsoft and CTS to establish an affiliate tenant for their subdomain (agy.wa.gov) federated with the wa.gov instance
• Agencies administer their affiliate tenant, including their own licenses
How This Will Work

• Synchronization of Exchange and Lync attributes will be restricted until, and if, these enterprise services move to the enterprise tenant

• Affiliate tenants are limited to their own subdomain namespace – they will have no access to the GAL or other agency directory information

• If an agency chooses to turn on these services in their own tenant, these will be isolated to their own namespace – again, no GAL

• This approach does not represent additional cost to O365 license purchasers
Beyond This Project

• Azure Active Directory Premium offers features that align with our planned Identity Management initiative – self-service password reset, group-based access management and provisioning, multi-factor authentication...

• CTS has begun conceptual design discussions with Microsoft to better understand this cloud-based service and its usefulness