

ITS Strategic Roadmap – FY16

Identity and Access Management

Author: *John Griffey*

Date last updated: *1/25/2015*

Background

The Metropolitan Government has standardized on Identity and Access solutions to ensure security throughout Metro. These solutions allow for users to securely log into the Metro network, access information and allow Metro to better and more efficiently secure the devices used by Metro departments.

The tools used in this mature space include Microsoft Active Directory Domain Services (ADDS), Microsoft's Domain Name Services (DNS) for internal and external DNS management, group policies and Active Directory Certificate Services (ADCS) which is used for the Metro Private Key Infrastructure (PKI).

Metro ITS is responsible for maintaining the overall health of the Active Directory Domain Services infrastructure. However, there are currently multiple Microsoft Active Directory domains across what is generally considered to be Metropolitan Government departments and agencies:

- Metro ITS provides Active Directory Domain Services, DNS services, group policy management, and Active Directory Certificate Services for Metro general government department employees, primarily those that are under the executive branch, but also a number of elected officials including the Davidson County Clerk, Property Assessor, Trustee and Register of Deeds.
- The Davidson County Sheriff's Office (DCSO) provides Active Directory Domain Services and group policy management and support for Sheriff's office staff. Metro ITS provides DNS support and Active Directory Certificate Services for DCSO.
- The Justice Integration Services (JIS) department provides Active Directory Domain Services and support for staff of the various judicial agencies, including Criminal Court Clerk, General Sessions, Chancery Court, District Attorney, and others. Metro ITS provides DNS support and Active Directory Certificate Services for all of these agencies.
- The Metro Nashville Public Schools (MNPS) fully supports their own Active Directory Domain Services, DNS, group policy and certificate services infrastructures.

These services are used by all of Metro and are "foundation" services, key to the business processes used by departments. With such a wide array of customers, the team's focus is on reliability, consistency and ever-increasing capability when it comes to the solutions and services provided.



Current Strategic Drivers

1. **Use of external cloud-based services requires robust identity systems** (Game Changing) – Continued emphasis on “identity” and the impact of dealing with external parties, such as MNPS, and cloud service providers, such as Microsoft, will drive the need to develop some level of federated services around identity.
2. **Demand for Secure Government Systems** (High) – With massive data breaches in the news on seemingly a daily basis, we must strive at all times to protect the security, availability and integrity of all data entrusted to our management.
3. **Customer desire for Self Service** (High) –Customer driven and a method of reducing workload on help desk by providing secure method of self-service password resets and the ability for departments to provision their own user accounts and security groups.
4. **Customer Need: support alternative authentication methods** (High) – Network devices, including wireless devices, require the use of TACACS+ and RADIUS for user and device authentication.
5. **Customer Need: streamlined authentication methods** (High) – Some applications are not capable of supporting Active Directory for authentication and require their own login. Customers have asked for single sign on capability, which would allow reduce the need to remember these multiple passwords.

On the Horizon Strategic Drivers

1. **Government Mandate: deploy DNSsec** (High) – Federal Government has mandated all federal agencies use DNSsec as a method of securing Domain Naming Services (DNS). Industry believes these mandates will be required of state and local governments in the next few years.
2. **Technology Change: Industry push to the use of advanced\multi-factor authentication methods** (High) –Identity industry projects an emphasis on providing alternative means to authenticate identity as well as the need for dual factor authentication and/or location based authentication solutions to strengthen the security of this service.

Short Term Goals (0-6 months) 7/1/15 – 12/31/15

#	Goal/Objective	Est. Start	Est. Duration
1	Deploy self-service password reset solution for enterprise.	7/15	6 months
2	Upgrade Active Directory Domain/Certificate Services to newest version.	7/15	6 months
3	Research the use of Active Directory Federated Services to provide identity solutions that would reach outside of Metro.	7/15	5 months
4	Research, purchase and implement RADIUS and TACACS+ authentication solution for use by the network team.	10/15	4 months
5	Research, purchase and implement DNSsec implementation.	7/15	3 months



Medium Term Goals (6-18 months) 1/1/16 – 12/31/16

#	Goal/Objective	Est. Start	Est. Duration
1	Begin Phase one for the Provisioning Project (planning for user provisioning), which would also help facilitate single sign on and multi-factor authentication. Capital funding will be required.	1/16	6 months

Long Term Goals (18-36 months) 1/1/17 – 6/30/18

#	Goal/Objective	Est. Start	Est. Duration
1	Begin Phase two for Provisioning Project (implementation).	1/17	12 months
2	Research Data Rights Management (DRM) solutions such as Active Directory Rights Management.	11/17	12 months

Related Roadmaps:

- Network Security
- Server Infrastructure
- Email and Calendaring
- Unified Communications

