	Georgia Technology Authority	
Title:	**Active Directory**	
PSG Number:	SA-03-009.01	**Topical Area:** App Development / Enabling Solution Use
Document Type:	Standard	**Pages:** 9
Issue Date:	1/15/03	**Effective Date:** 1/15/03
POC for Changes:	GTA Infrastructure Services	
Synopsis:	Specifies the Active Directory (AD) requirements, topology and design.	

PURPOSE

To define an effective, scalable, secure and manageable Active Directory**™** forest design and to facilitate one standardized infrastructure for the State's Active Directory**™** which will reduce multiple sign-ons and reduce total cost of ownership for the State's network operations. The Georgia Technology Authority (GTA) shall govern the implementation and operation of Microsoft's Active Directory™ on the State's enterprise network.

SCOPE

This standard applies to any Agency's implementation of Active Directory**™**. This standard covers implementation of any Active Directory**™** forest established on the State's enterprise network within a production environment. Although there are touch points between Active Directory™ and the Georgia.Gov Domain Naming Convention the two are not directly related.

STANDARD

Agencies, Political Subdivisions, and other entities participating in the State's Active Directory™ shall comply with all Active Directory™ prescribed standards, processes, and specifications defined by the Georgia Technology Authority. GTA will develop specific procedures and sub-process that Agencies will follow to implement Active Directory™.

1. Structure

The initial design is structured to take advantage of the flexibility of domains and Organizational Units (OUs) in Active Directory™. An empty forest root is implemented to maximize security of the forest root; allow child domains to be reorganized, as necessary; and recognize the differing roles among the GTA, Agencies, and the Outsource Vendor. A single forest design is employed to reduce total costs, create a single Exchange 2000 organization, and ease administration. A single accounts domain is utilized to create a simple administrative structure for the Outsource Vendor. Resource domains are used to separate administration of systems maintained by their respective agencies. Top-level Organizational Units (OUs) are created for each state agency in the accounts domain to allow application of separate group policy objects. All OU designs are governed by the Organizational Unit Standard and must be approved by the GTA.

2. Single Forest

There is one enterprise forest structure for the State of Georgia, with justified exceptions. GTA is responsible for the availability of the State Forest infrastructure for Active Directory™ services and will retain control of the Forest Root Domain. GTA will be responsible for maintaining Active Directory™ services to ensure business continuity for each Agency.

Requests for enterprise Schema modifications and security policy changes must be approved by GTA.

3. Domain Plan

There will be a single, dedicated root domain for any/all forests. This will provide a controlled environment for forest wide change management and limit the amount of replicated data. The root domain will contain no user accounts and will be used strictly as an empty domain to manage the schema, global catalog, site topology, security and enterprise policy.

GTA will be responsible for the operation of the enterprise forest root domain.

Each Agency shall have the option of its own domain under the enterprise forest root domain. Based on business requirements and upon approval of GTA, Agency sub domains may be created.

All sub-domains established beneath the State's enterprise domain will be owned by the Agency and the Agencies will oversee management of their domains in compliance with current State Active Directory™ Standards. These sub-domains will be established within the State's single Forest as defined in the Forest Standard. The Agency domains will contain Agency owned and operated Web, Application, Databases servers and their respective administration accounts to maintain these servers only.

There will be one accounts domain that is administered by the outsourced vendor. Each agency will have an Organizational Unit (OU) structure within this domain that will contain the Agencies users, computers, file and print servers. The Agencies will manage their OU through the outsourced vendor.

4. Domain Control and Security

Membership in the dedicated enterprise forest root domain Schema, Enterprise and Domain Administration groups is restricted and controlled by GTA and implemented by GTA. GTA will maintain a high level of security on all levels to ensure only properly authorized changes are implemented.

5. Domain Name Service (DNS) Zones

The primary DNS zone for the State of Georgia is owned and managed by GTA. DNS support for Active Directory™ for the State appears as a sub zone and is replicated between all DNS servers in the dedicated enterprise forest root domain. Agencies may create and manage sub zones to the Active Directory™ zone in accordance with GTA prescribed standards. All DNS zones will be implemented as Active Directory™ integrated zones where possible.

6. Organization Unit (OU) Plan

Each Agency manages its objects in the directory, while the Georgia Technology Authority manages the configuration of the directory service. The Agency is responsible for completing an initial OU design and submitting it to the GTA for approval.

7. Organizational Control

The domain owner is responsible for the management of all Organizational Units and submission of requests for creation of all its Organizational Units within its sub-domain and its high level OU in the Accounts domain.

8. Organizational Ownership

The (Agency’s) sub-domain owner designates an Organizational Unit owner for each Organizational Unit. Each Organizational Unit owner is a data manager with control over a sub-tree of objects in Active Directory**™**. The sub-domain owner controls the operation of the service.

9. Sites Plan

The Site Plan defines an Active Directory™ site as a set of well-connected Internet Protocol (IP) subnets, equivalent to Local Area Network speeds or greater.

All sites are to be designed by the Agency or Agencies affected in conjunction with the GTA and the outsource vendor. Agencies' will design a site topology that reduces Wide Area Network (WAN) utilization during Active Directory™ replication and client logon. The Agency or Agencies affected are responsible for the submission of the site topology design to GTA.

10. Site Control

The Agency's responsibilities include advice and consent on the following:

- Changes to site topology
- Location of domain controllers

11. Backup and Disaster Recovery

Backup and recovery of the forest root domain will be the sole responsibility of GTA.

12. Active Directory™ Replication

Replication of the enterprise forest root domain will be the responsibility of GT A and will be implemented as Active Directory™ integrated zones where possible.

13. Active Directory™ Domain Naming

The name of each sub-domain under ad.ga.gov will consist of the acronym that has been selected for the Agency (i.e. DHR.AD.GA.GOV). There will be one Accounts domain (Accounts.ad.ga.gov) that will contain all user computers, file and print servers.

The Outsource Vendor shall assign workstation names of length of 15 hex characters. Workstation names must be specified on asset tag unless a security risk dictates otherwise. Workstation names must be available via Web access to include information for application help and on asset tag. Consideration is given to using asset management software.

Domain Naming shall include organization acronym, followed by State Root Domain placeholder (i.e. DHR.AD.GA.GOV). Maximum values apply and should not exceed 15 characters. No special characters shall be used.

Servers shall be named with a string containing a maximum of 15 characters and constructed as follows (working from the left): An agency code of 3 or 4 characters that is managed by the GTA; followed by a two character function code that is managed by the GADAC; next a 3 digit sequence number assigned by the outsource Vendor; A hyphen; A 5 or 6 character optional description code as managed by the Agency. The Agency can indicate here, e.g., whether the server is production or development. The string shall not contain blanks or special characters.

Sites shall be named with a string containing a maximum of 255 characters and constructed as follows (working from the left); The city name, a hyphen, and the site description. The string shall not contain blanks or special characters.

The User login name/User Principal Name (UPN) is formatted as first initial, full last name @ organizational acronym, followed by the State Root Domain name (i.e. jdoe@gta.ad.ga.gov). Length and duplicate handling follow the NetBIOS login name definition. NetBIOS login name or Pre-Windows 2000 login name would reflect first initial, full last name and follow the conventions below. The total number of characters shall not exceed 15; truncate within last name to avoid using more than 15 characters. Duplicates should be handled by the following in sequence; add middle initial, add next letter of first name, append a sequence number if still not resolved. User accounts require the following attributes be filled in using the following formats; First Name, Last Name, and Initials. The display name is formatted as Last name, First name followed by agency acronym for duplicate display names. If there are duplicates even with agency acronym add division or other identifier to eliminate duplicates. Examples would be Smith, John – Smith, John (DHR) – Smith, John (DHR-DFCS) Address City, State, Zip Code, Company to contain the GTA maintained Agency codes, Department to contain agency division or work group as defined by each agency, Office Phone number, and E-mail address. Manager must be populated if present on E-form. Other phone/pager/fax numbers must be populated if present on the E-form.

Administrative accounts are formatted as follows. The User login name/User Principal Name (UPN) is formatted as “!”, first initial, full last name (*see note) @ organizational acronym, followed by State Root Domain name. For example !jdoe@gta.ad.ga.gov. The “!” prefix indicates an administrative account. The total number of characters should not exceed 15; truncate within last name to avoid using more than 15 characters. Duplicates should be handled by the following, in sequence, add middle initial, add next letter of first name , append a sequence number if still not resolved. User accounts require the following attributes be filled in using the following formats, First Name, Last Name, Initials – may be blank if person does not have middle initial, Display name – formatted as Last Name, First Name followed by agency acronym for duplicate display names. If there are duplicates even with agency acronym add division or other identifier, eliminate duplicates. Examples would be Smith, John – Smith, John (DHR) – Smith, John (DHR-DFCS), Address, City, State, Zip Code, Company to contain the GTA maintained Agency codes, Department to contain agency division or work group as defined by each agency Office Phone number, and E-mail address. Manager must be populated if present on E-form, other phone/pager/fax numbers must be populated if present on the E-form User Login Name/User Principal Name.

Service Accounts should begin with “**svc-**“agency code prefix (e.g., dot) followed by a hyphen and a name that describes the service it supports (e.g., Svc-dot-Meterman). The Description should contain the ID of the owner/requestor of the service account. The account options **User cannot change password** and **Password never expires** should be selected. Service accounts should be a member of Domain Guest Security Group, unless there is a process justification for membership in Domain Administration. No service account should be a member of Domain Users or any other User Global Group, unless there is a specific process justification.

User E-mail Address Standard format is as follows; First initial, full last name (*see note) @ agency code, followed SMTP domain name, which should reflect “First Initial and full lastname@Organization agencycode.GA.GOV, for example jdoe@gta.ga.gov.

*Total number of characters cannot exceed 15; truncate within last name to avoid using more than 15 characters. Handle duplicates and described above.

Generic E-mail Addresses Standard format is as follows; Agency code, hyphen, Department acronym, optional hyphen, optional custom field (i.e. gta-hr-resumes@gta.ga.gov). Mail enabled accounts may be created and then disabled to keep users from logging on the domain with the account.

Application Naming Standard format is as follows; Vendor name acronym, hyphen, product name acronym, hyphen, version, optional hyphen, and optional custom field (i.e. MS-PROJECT-2000-SR1). An application team will develop a list of Vendor acronyms for use in application group object naming conventions.

Group Policy Object Naming Standard format is Agency code, hyphen, business function or location, hyphen, and agency defined optional field.

Printer Naming Standard format is as follows; Agency code (4 characters), “P”, Printer ID (5 digits) for example, GDOTP12345. The location field is required and should contain a standardized code. Codes must be standardized by the outsource vendor, i.e., Building Acronym/Code, hyphen, Floor, hyphen, Division, hyphen, Asset/Inventory Number, followed by fields for Location (room/cube) and Comment (description). A comment field is required and shall include information as determined by the individual agency.***Note:** Model attribute must be populated.

In cases where the server is multi-functional, the highest priority function takes the name, e.g., a combined domain controller and WINS server will be coded as DC.

Server Function Codes

Anti-virus Server	AV
Application Server	AP
Database Server	DB
Development Server	DV
DHCP Server	IP
DNS Name Server	NS
Domain Controller Server	DC
File Server	FS
Gateway Server	GW
Mail/Messaging Server	MS
Print Server	PS
Proxy Server	PX
Remote Access Server	RA
Remote Installation Server	RI
System Management Server	SM
Terminal Server	TS
Utility ("catchall") Server	UT
Web Server	WW
WINS Server	WN

14. Domain Name Service Servers

All Windows 2000™ dynamic DNS servers shall be located behind a firewall.

15. Availability

There will be at least three domain controllers for the root forest directory. One copy of a full backup of the forest root will be made daily. (Note: AD backup must be enabled at the forest root.) One copy of the tape will be retained for 35 days at an offsite location. The tape expires after 45 days; Tape access is limited to authorized personnel. An approved disaster recovery plan must be in place. The plan should include “mission critical” agencies at a minimum. The plan should include scenarios for; No equipment; No equipment and no people; No access to equipment. The plan must be tested at least once a year, without prior notice to the recovery team. The plan must include a specified offsite location that meets industry standards for disaster recovery. An overall summary report of AD status (including backup status) must be available to authorized personnel for viewing at any time. A full detailed report must be available upon request.

16. Auditability

Logs must be maintained for a minimum of 6 months. Logs will be available to internal auditors. Exception reports from the logs will be reviewed daily and a report of summary of exceptions will be available to designated agency representatives. Logs must be replicated hourly to another location that is accessible only by executive-level security personnel. Logs should be renamed during the replication process to prevent overwriting in the replicated location. Log size should be set according to need, so that events within the last 60 days are easily accessible from the primary log file. The outsource vendor will provide a list of *resources against current user access levels* at least once a year and on demand by the agencies. The outsourced vendor will respond to log file inquiry requests within 2 business days, and provide weekly reports of failed login attempts to agency designee. The vendor will notify the affected agency immediately of repeated failed attempts. Events to be Logged includes Success and Failure Auditing for logins at the root forest level and/or where all user accounts are located, success and failure auditing for Object Access at the domain level, all user account changes (e.g., passwords), and schema modifications. There will be internal auditors. Agencies and auditors will have *view of only* privileges for OUs in the accounts domain.

AUTHORITY

O.C.G.A. §§ 50-25-4(a)(15), (21), (29).

EXCEPTIONS

Requests for variance and exceptions to this standard must be submitted to the State CIO.

RELATED ITEMS

See Domain Naming Policy

GUIDELINES

For further details, please refer to the Georgia Digital Academy Report on Active Directory, entitled, Streamlining Directory Services in Georgia Government: An Enterprise Approach, which can be found at gta.georgia.gov under Technology Initiatives > Digital Academy.

Note: The ideas and expressions contained within Digital Academy Reports are those of the individual authors and do not necessarily reflect the positions and policies of the Georgia Technology Authority.

TERMS AND DEFINITIONS

Domain: In Windows 2000 and Active Directory, a collection of computers defined by the administrator of a Windows 2000 Server network that share a common directory database. It provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains.

Schema: The definition of an entire Active Directory™ database; the universe of objects that can be stored in the directory is defined in the schema. For each object class, the schema defines what attributes an instance of the class must have, and what object class can be a parent of the current object base.

Domain Name Service: Domain Name Service (DNS) is a hierarchical distributed database used for name/address translation and client server rendezvous. Domain Name Service is the namespace used on the Internet to translate computer and service names into TCP/IP addresses. Active Directory™ uses DNS as its location service which enables clients to find domain controllers using DNS queries.

Georgia.gov: The State of Georgia has registered the georgia.gov second level domain name with the General Services Administration. Georgia.gov will be used as the primary domain for the State of Georgia's enterprise portal. Additionally, mygeorgia.gov, ga.gov, and myga.gov second level domain names are registered to the State of Georgia. Mygeorgia.gov and myga.gov are slated for use with the personalization component of the portal. Ga.gov is reserved for future use. Ga.gov is used as a parent domain to ad.ga.gov which is the root for the active directory name space. The Georgia Technology Authority is the trustee for managing the registration of third and fourth level domains associated with georgia.gov, mygeorgia.gov, ga.gov, and myga.gov second level domain names.

Sub-Domains: Any child of a domain zone.

Site: A site is defined as one or more well connected TCP/IP subnets.

Note: The PSG number was changed from S-03-009.01 on September 1, 2008.