Introduction on IAM

What’s posted on this monitor?

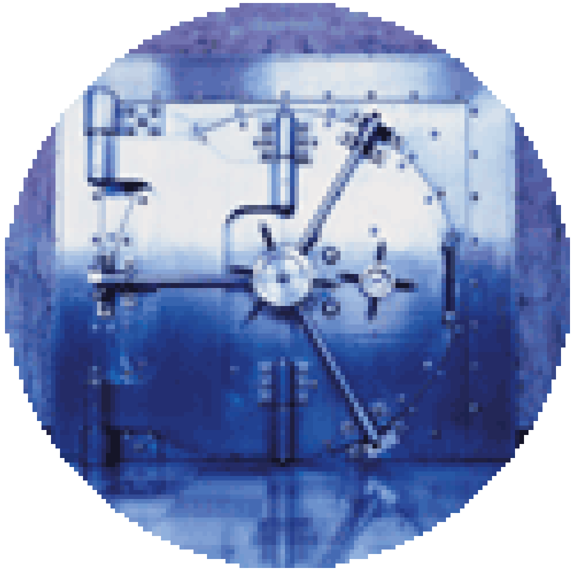
a – password to financial application

b – phone messages

c – to-do’s

Challenge: Managing Security Risks

- Majority of security breaches from within organization
- Fragmented security policies
  - Orphaned accounts
  - Expired access rights
  - Lack of aggregated audit and accountability
- Leaked passwords, social engineering
- Manual provisioning requests prone to errors
- Network administrators unaware of organizational and role changes



Today’s IT Challenges

More Compliant Business

- Increasing regulatory demands
- Increasing privacy concerns
- Business viability concerns

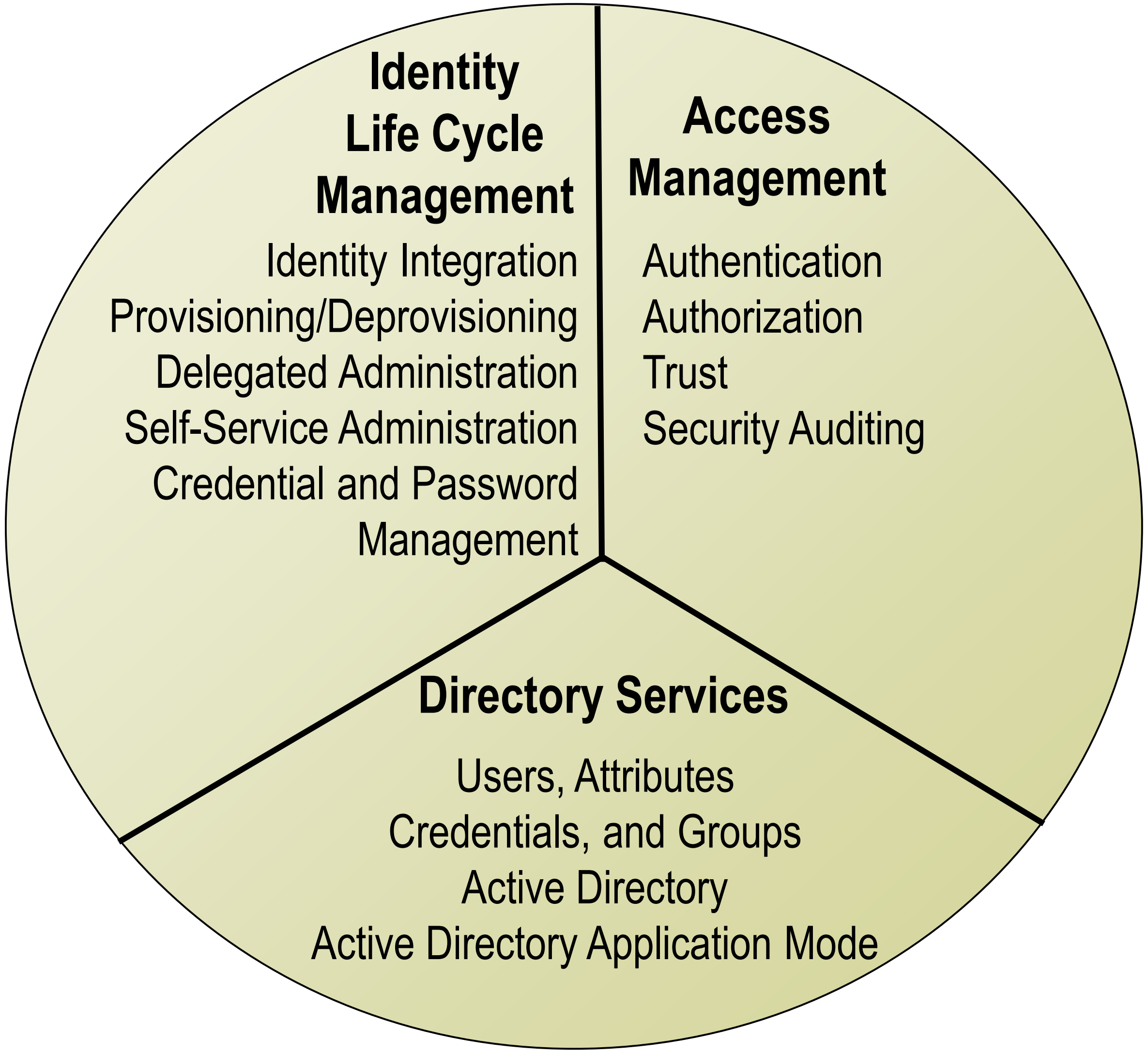
More Secured Business

- Organized crime
- Identity theft
- Intellectual property theft
- Constant global threats

More Agile Business

- More accessibility for employees, customers and partners
- Higher level of B2B integrations
- Faster reaction to changing requirements

Understanding Identity and Access Management Basics



Identity Life Cycle Management

Identity Integration
Provisioning/Deprovisioning
Delegated Administration
Self-Service Administration
Credential and Password Management

Access Management

Authentication
Authorization
Trust
Security Auditing

Directory Services

Users, Attributes
Credentials, and Groups
Active Directory
Active Directory Application Mode

Control Physical and Logical access to Assets

- Access controls can be implemented at various layers of a network and individual systems
- Some controls are core components of operating systems or embedded into applications and devices and some with third-party add-on packages
- Different controls provide different functionality, they should all work together to keep the bad guys out and the good guys in
- Companies do not want people to be able to walk into their building arbitrarily, sit down at an employee’s computer, and access network resources.
- Companies also don’t want every employee to be able to access all information within the company, as in human resource records, payroll information, and trade secrets.
- Companies want some assurance that employees who can access confidential information will have some restrictions put upon them

Access Control Layers

Access control consists of three broad categories: administrative, technical, and physical. Each category has different access control mechanisms that can be carried out manually or automatically.

Administrative Controls

- Policy and procedures
- Personnel controls
- Supervisory structure
- Security-awareness training
- Testing

Physical Controls

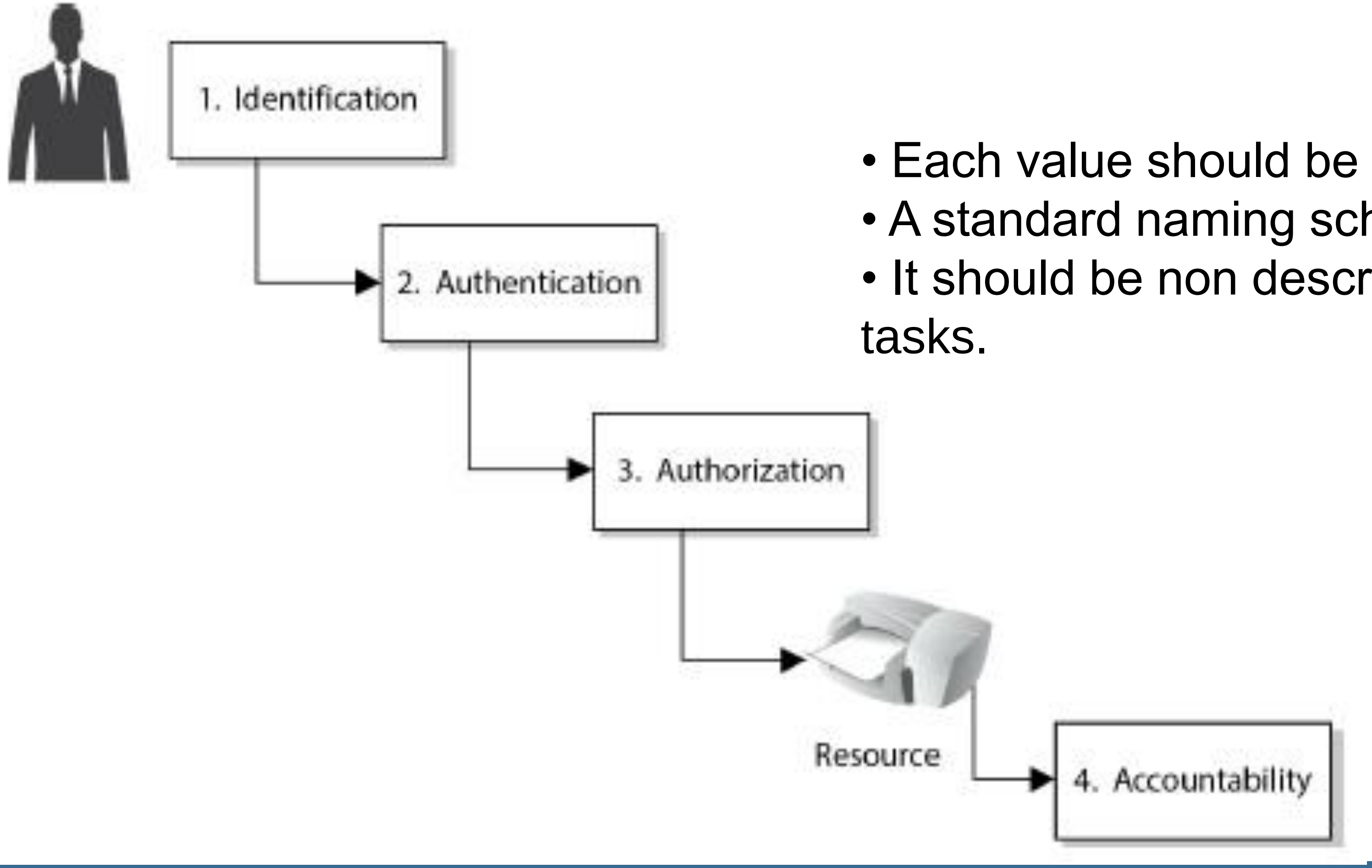
- Network segregation
- Perimeter security
- Computer controls
- Work area separation
- Data backups
- Cabling
- Control zone

Technical Controls

- System access
- Network architecture
- Network access
- Encryption and protocols
- Auditing

Identify Definition

- Identification is the first step for a subject to access an object
- Identification describes a method by which a subject (user, program, or process) claims to have a specific identity (username, account number, or e-mail address).
- An individual's identity must be verified during the authentication process

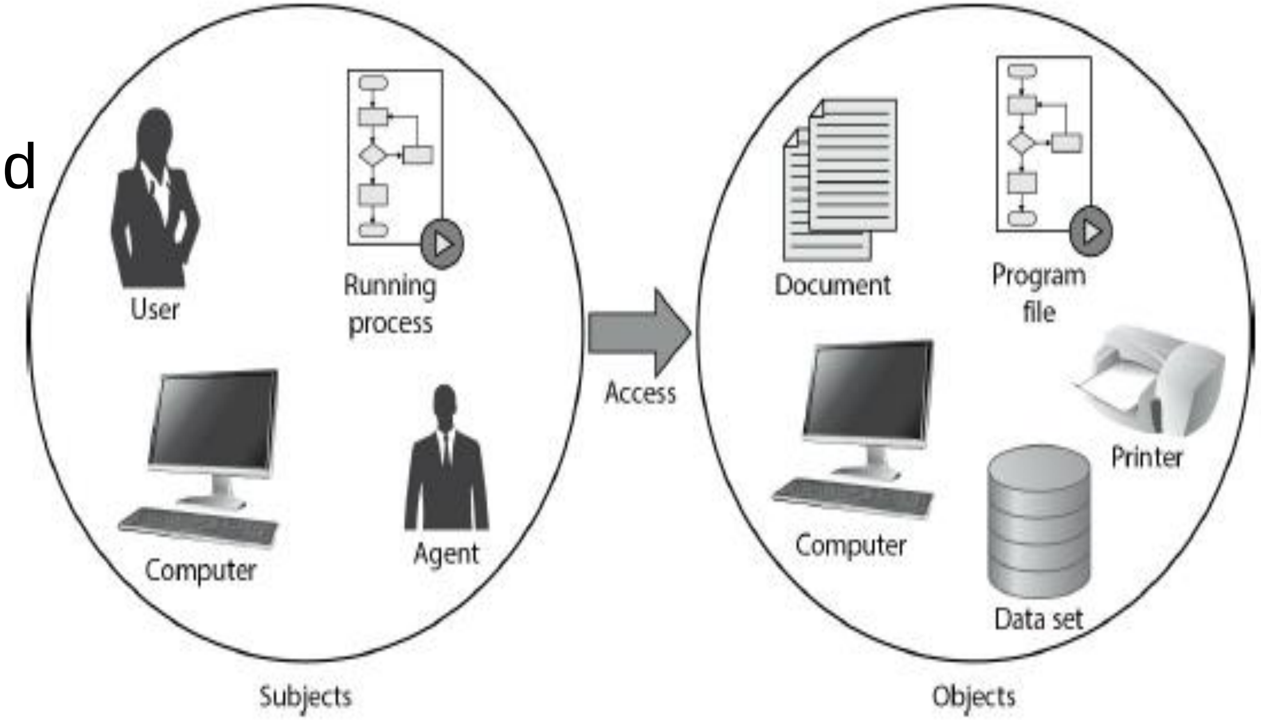


- Each value should be unique, for user accountability.
- A standard naming scheme should be followed.
- It should be non descriptive of the user's position or tasks.

Access Controls

Access is the flow of information between a subject and an object.

- Subject: Active entity that can access objects
  - a process representing user/application
  - often have 3 classes: **owner**, **group**, **world**
- Object: Passive Entity or access controlled resource
  - e.g. files, directories, records, programs etc
  - number/type depend on environment
  - Contains information or functionality
- Access right: way in which subject accesses an object
  - e.g. read, write, execute, delete, create, search



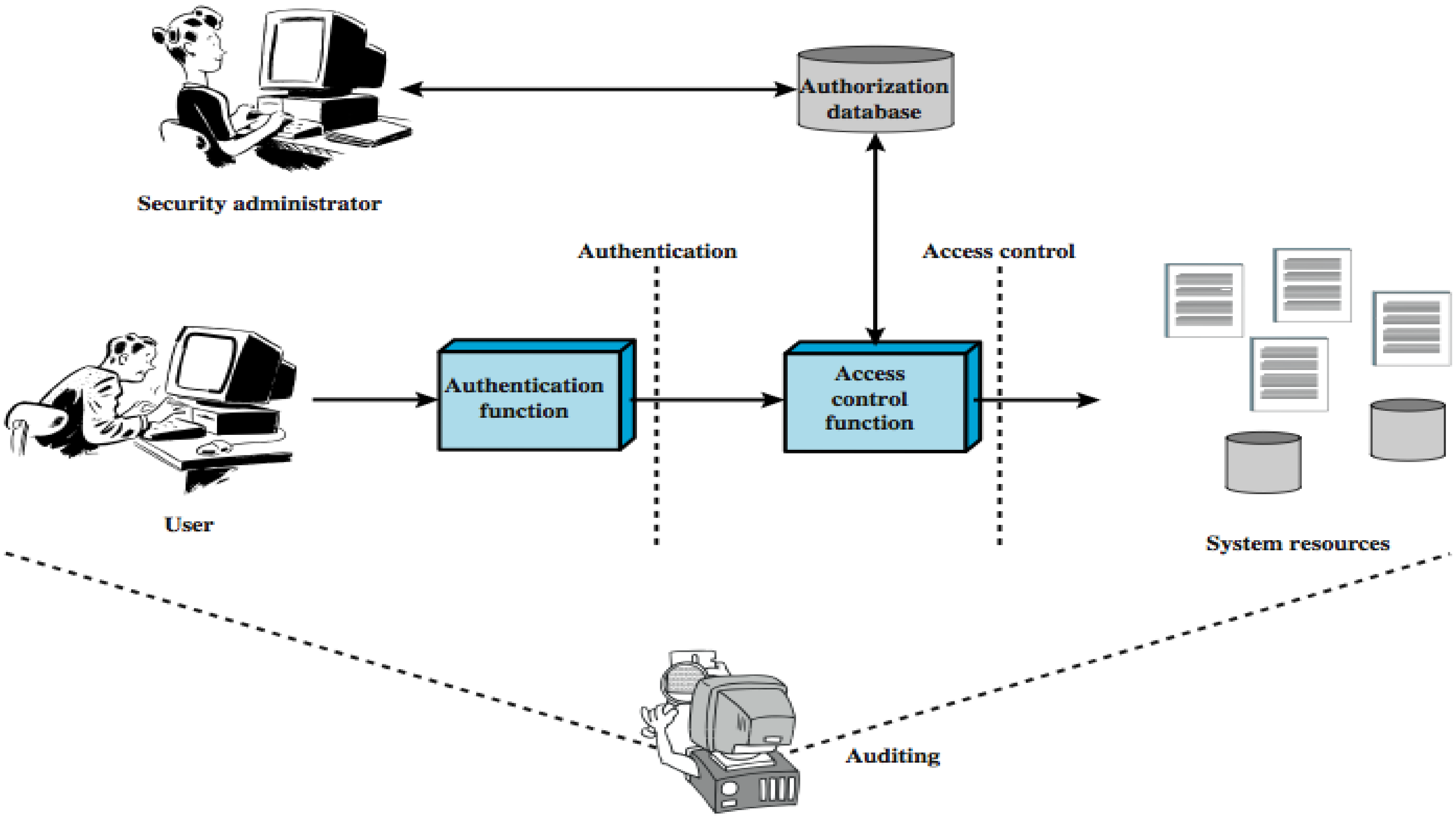
Access Control

- Access control is usually taken care of in three steps, which are identification, authentication, and authorization
- Access control is extremely important because it is one of the first lines of defense in battling unauthorized access to systems and network resources.
- The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner
- Access controls give organizations the ability to control, restrict, monitor, and protect resource availability, integrity, and confidentiality.
- The more sensitive or valuable the information, the stronger the control mechanisms should be
- Assume have users and groups
  - authenticate to system
  - assigned access rights to certain resources on system

Challenges in Access Control

- Various types of users need different levels of access
  - Internal users, contractors, outsiders, partners, etc.
- Resources have different classification levels
  - Such as confidential, internal use only, private, or public
- Diverse identity data must be kept on different types of users
  - Credentials, personal data, contact information, work-related data, digital certificates, cognitive passwords
- The corporate environment is continually changing

Access Control Flow



Basic Access Control Practices

- Deny access to systems by undefined users or anonymous accounts
- Limit and monitor the usage of administrator and other powerful accounts
- Suspend or delay access capability after a specific number of unsuccessful logon attempts
- Remove obsolete user accounts as soon as the user leaves the company
- Suspend inactive accounts after 30 to 60 days
- Enforce strict access criteria
- Disable unneeded system features, services, and ports
- Enforce the need-to-know and least-privilege practices
- Replace default password settings
- Ensure that logon IDs have nothing to do with job function
- Enforce password rotation and requirements such as length, contents, storage, and transmission

Access Control Requirements

- Reliable input: a mechanism to authenticate
- Fine and coarse specifications: regulate access at varying levels (e.g., an attribute or entire DB)
- Least privilege: min authorization to do its work
- Separation of duty: divide steps among different individuals
- Open and closed policies: accesses specifically authorized or all accesses except those prohibited
- Administrative policies: who can add, delete, modify rules

Types of Access controls

- **Discretionary** access control (DAC): based on the identity of the requestor and access rules
- **Mandatory** access control (MAC): based on comparing security labels with security clearances (mandatory: one with access to a resource cannot pass to others)
- **Role-based** access control (RBAC): based on user roles
- **Attribute-based** access control: based on the attributes of the user, the resources and the current environment

Directory

- Similar to your phone directory or Yellow pages
- For Example in Windows you login to Domain Controller that has hierarchical directory in its database. The database is running a directory service (Active Director.
- Directories Most enterprises have some type of directory that contains information pertaining to the company’s network resources and users.
- Most directories follow a hierarchical database format, based on the X.500 standard, and a type of protocol, as in Lightweight Directory Access Protocol (LDAP), that allows subjects and applications to interact with the directory.
- Directory service keep all of these entities organized using *namespaces*.

X.500 is a *standard* way to develop an electronic directory of people in an organization so that it can be part of a global directory

Lightweight Directory Access Protocol (LDAP) - Directory Services

- LDAP consists of a set of protocols developed to allow Internet clients to access the X.500 Directory using the TCP/IP networking stack
- LDAP defines an open, vendor-neutral, industry standard network protocol and set of access methods to a directory
- LDAP has become the standard access method for directory information on almost any system on an intranet and on the Internet.
- LDAP is currently supported in most network OSs, groupware, and Internet / Intranet applications
- Most directory services are accessed through LDAP
- Stores identity information
  - Personal Information
  - Attributes
  - Credentials
  - Roles
  - Groups
  - Policies

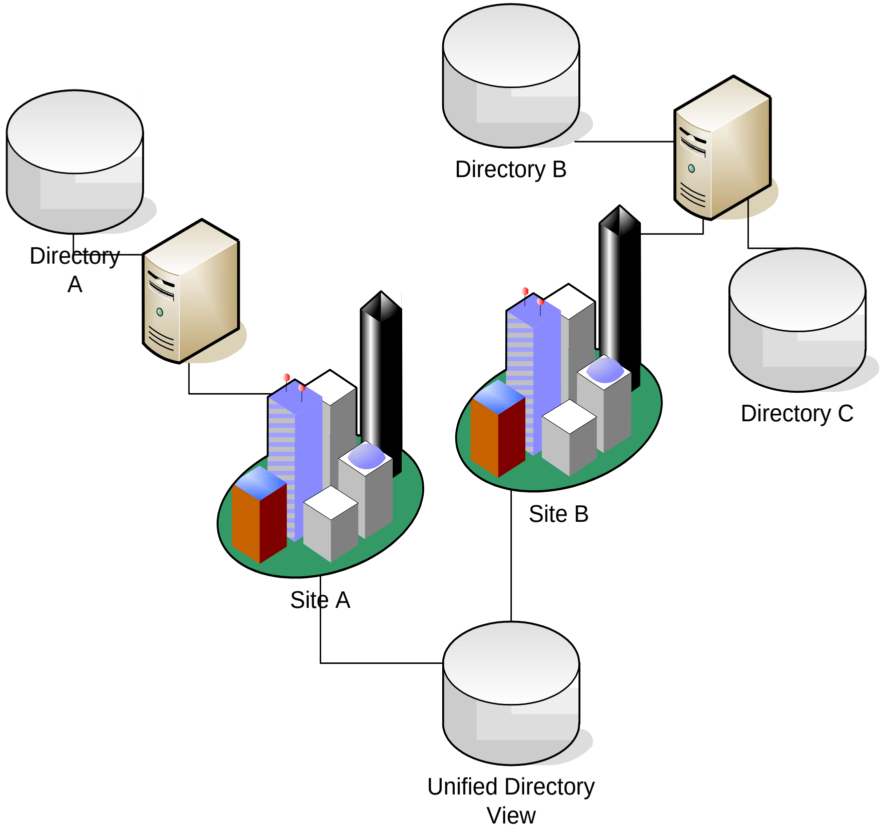
Directory Services

- Directory Servers are centralized repositories for storing and managing information in a hierarchical structure in the database (directory). i.e. provides Directory Services
- Directories can be searched by specific criteria or by predefined set of categories.
- Data searched (access) is frequent when compared to write (update)
- Types of Directories
  - Centralized – One Directory Server per location.
  - Distributed – Information can be partitioned or replicated across multiple servers which are distributed geographically.
- Information stored in Directory Server
  - Identity profiles & access privileges to information about application and network resources, printers, network devices and manufactured parts.
  - Information can be used for authentication and authorization of users to enable secure access to enterprise and Internet services and applications

Directory Services

In a database directory based on the X.500 standard

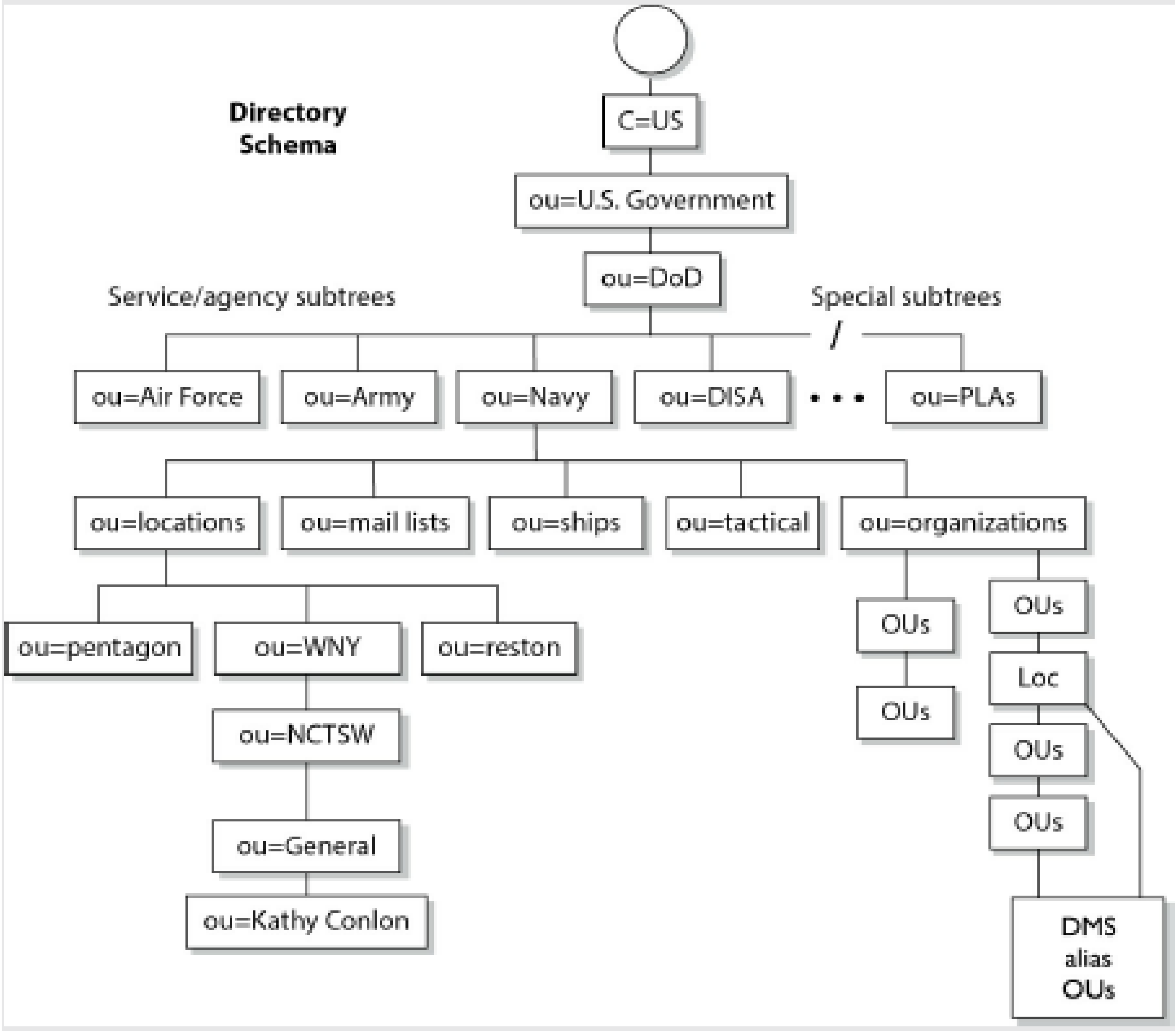
- The directory has a tree structure to organize the entries using a parent-child configuration.
- Each entry has a unique name made up of attributes of a specific object.
- The attributes used in the directory are dictated by the defined schema.
- The unique identifiers are called distinguished names.



Directory Schema

Directory schema describes the directory structure and what names can be used within the directory

The diagram shows how an object (Kathy Conlon) can have the attributes of ou=General, ou=NCTSW, ou=WNY, ou=locations, ou=Navy, ou=DoD, ou=U.S. Government, and C=US.



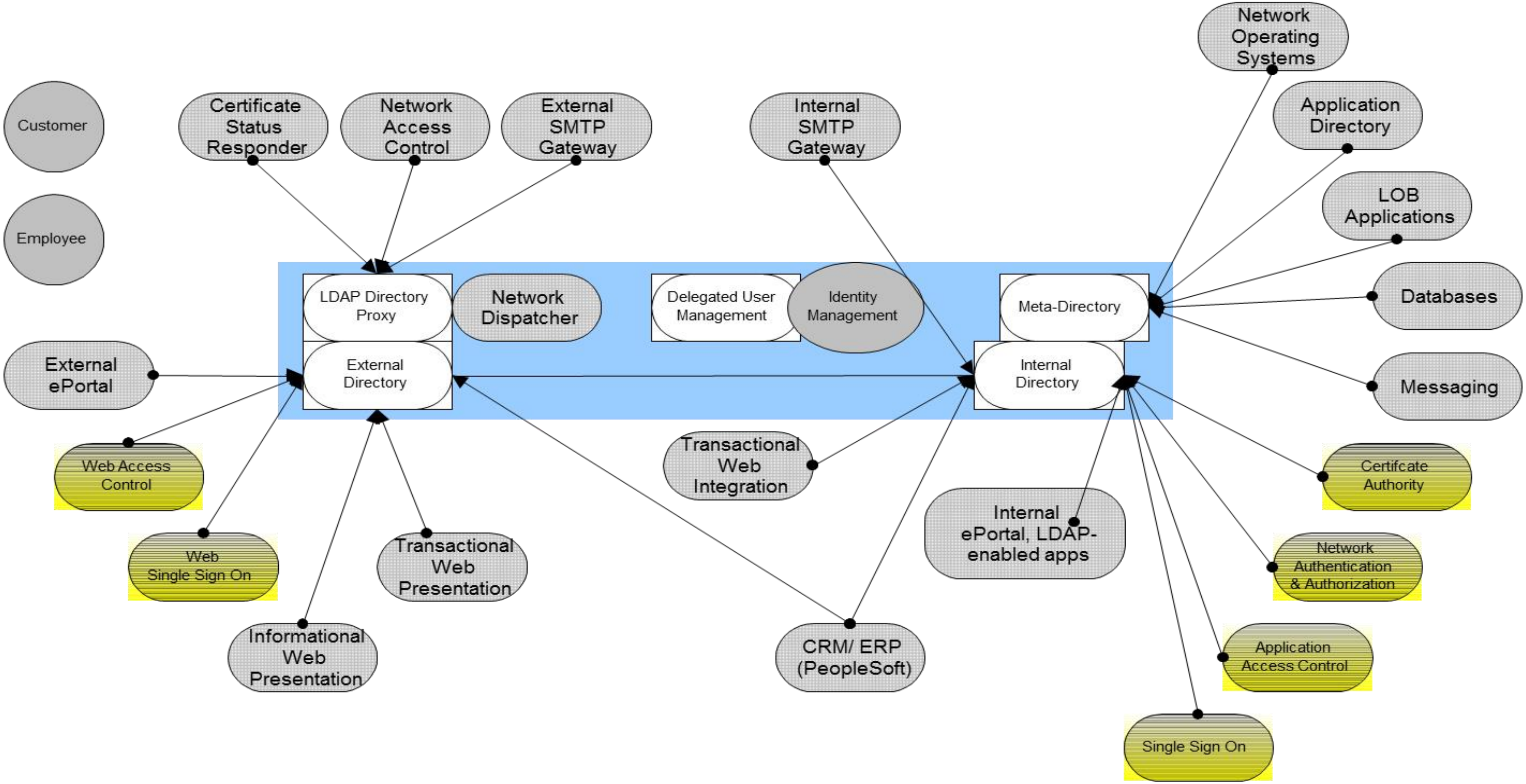
Directory Services Usage

- Directories are a critical infrastructure component
  - Identity repositories
  - Metadata replication/synchronization services
    - A meta-directory gathers the necessary information from multiple sources and stores it in one central directory
  - Directory virtualization
    - a virtual directory does not physically store the data but points to where the actual data resides
  - A virtual directory plays the same role and can be used instead of a meta-directory.

Directory Services Role in IAM

- A directory used for IAM is specialized database software It is the main component of an identity and Access management solution.
- Optimized for reading and searching operations.
- Resource information, users' attributes, authorization profiles, roles, access control policies, and more are stored in this one location.
- When other IAM software applications need to carry out their functions (authorization, access control, assigning permissions), they now have a centralized location for all of the information they need.

Sample Directory Management View – Enterprise Directory



Role of IAM in Enterprise

Identity & Credentials:

1. Centralizes identity flows and the on/off-boarding experience wherever possible to reduce risk, improve consistency, and minimize cost.
2. Enforces a common identifier for all personnel utilizing Organization assets, employee & non-employee
3. Automate the provisioning and de-provisioning of core credentials and roles tied to identity events.

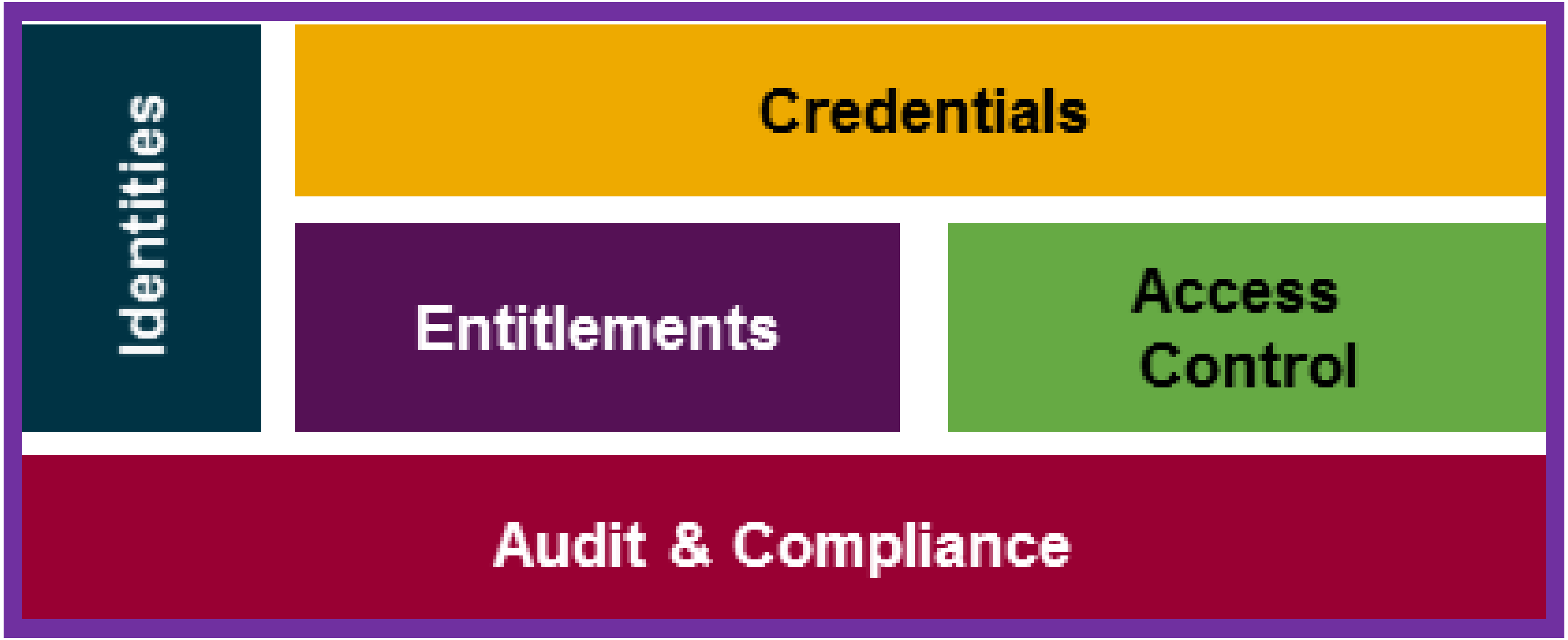
Entitlements and Access Control:

1. Implement a business application on-boarding paradigm (aka “adoption”) that enables targeted applications to integrate to IAM
2. Target high-risk applications (e.g. SOX/PCI), to be fully integrated to IAM with identity-event-driven JML process

Audit and Compliance:

1. Enable the business to perform scheduled or ad-hoc access reviews of all users and the access they hold
2. Provide accurate and timely compliance / auditing reports

IAM Program – Strategic Goals



Identities

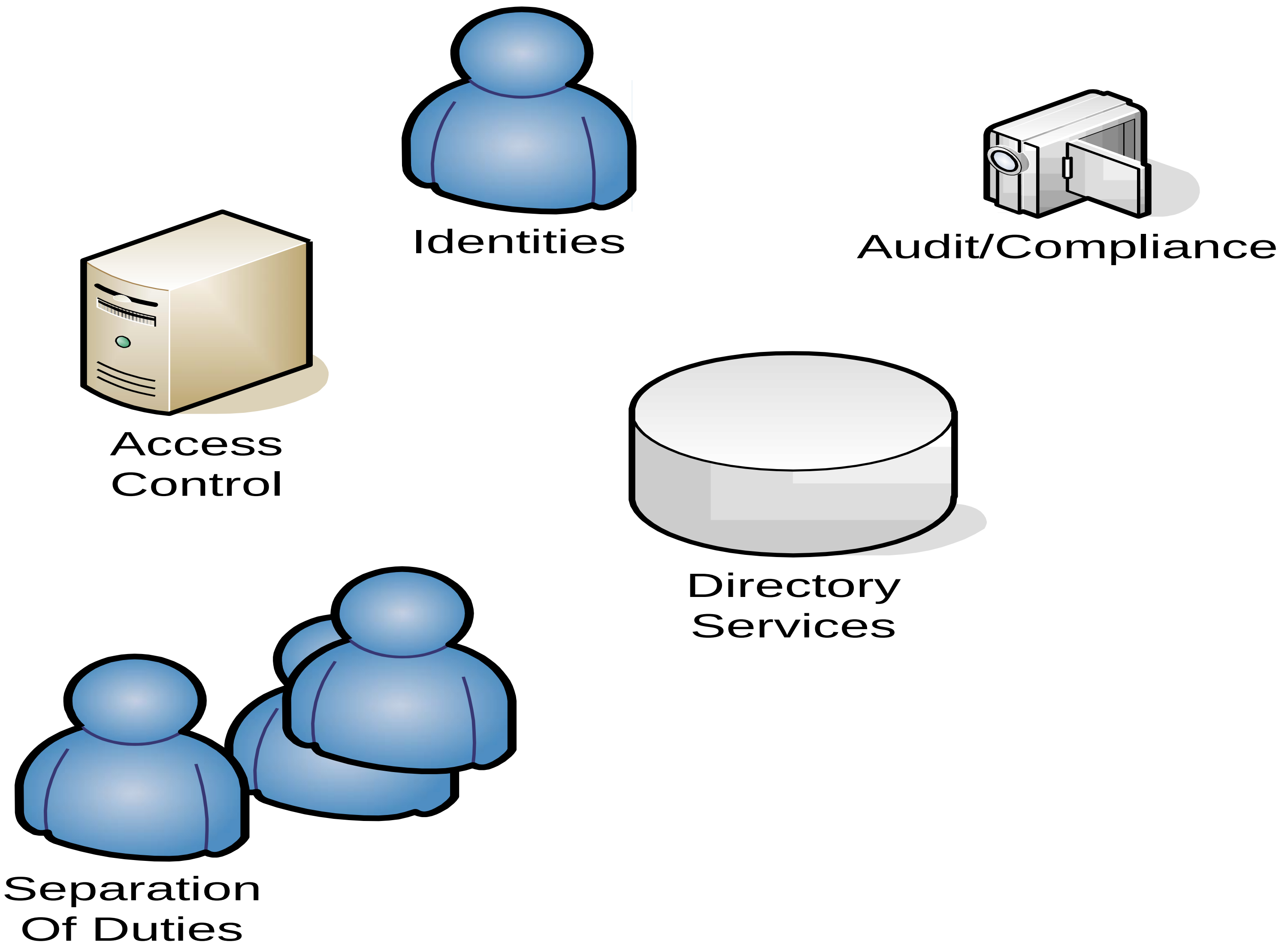
Credentials

Entitlements

Access Control

Audit & Compliance

Issues Addressed by Identity Management



Identities

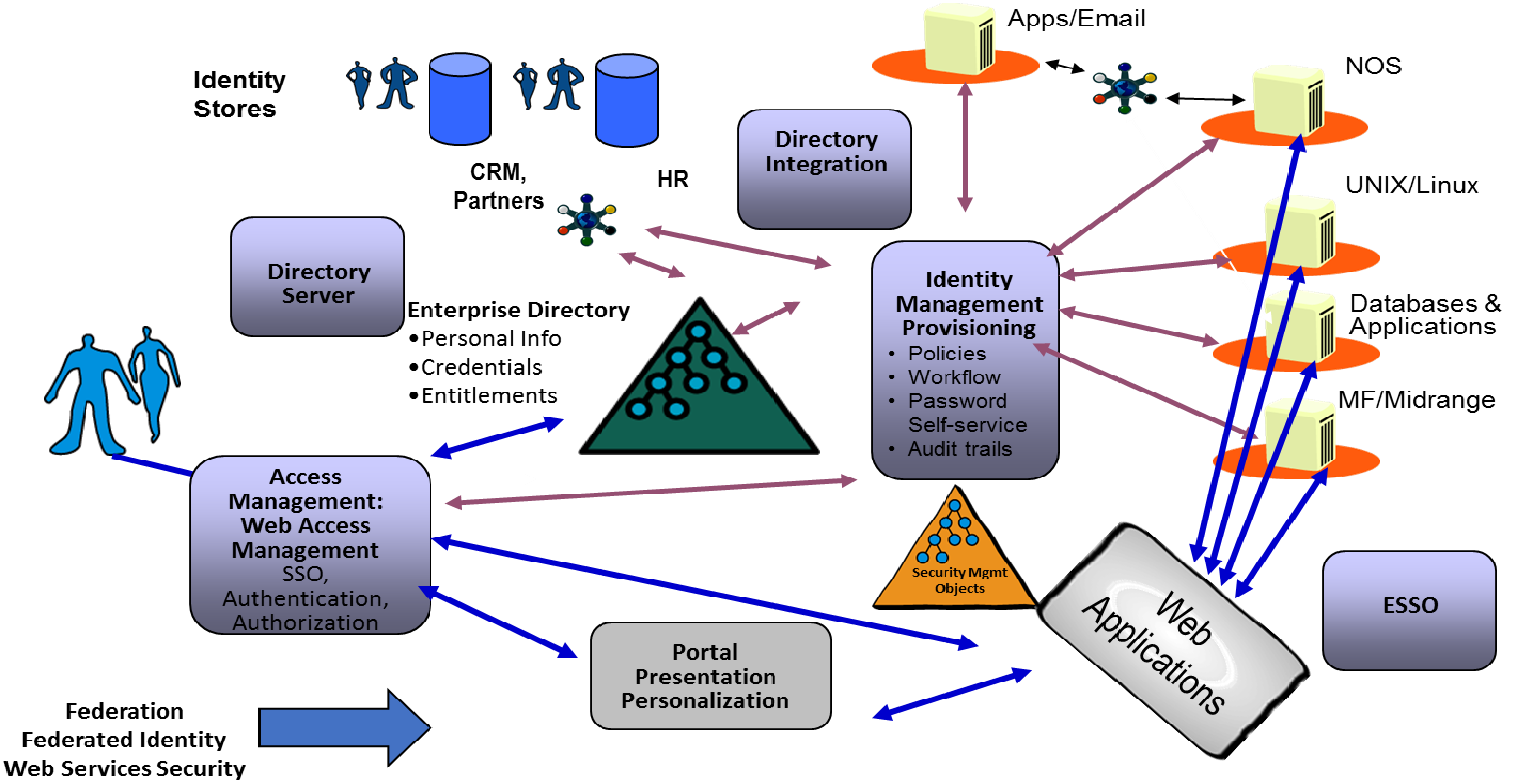
Audit/Compliance

Access Control

Directory Services

Separation Of Duties

Identity and Access Management Solution View



Popular Products

IBM

ca technologies

Microsoft

ORACLE IDENTITY MANAGEMENT

Ping Identity

okta

RSA SECURITY

Thank You