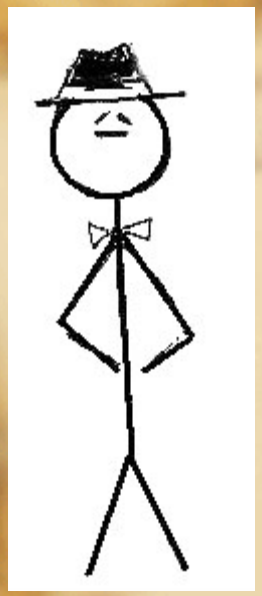


iamMCG

Identity and Access Management for Montgomery County Govt

Bala Vellaiappan

Roopa Suryanarayana

Suchitra Subbakrishna

Agenda

- IT Identity And Its Challenges
- IM Solution Architecture and Scope
- iamMCG
- What/How iamMCG Works
- Complex Scenarios
- Where are We; Where do We Go

Identity Management?

- Creating A Corporate Identity for a User
- Providing access to all IT Resources that the user is **Entitled** to
- Single Source of Mgmt for Password(s) for IT Resources
- Capabilities to Support Complex IM Business Processes
  - Promotions, Transfers, Temp-to-Perm, Retiring
- Real-time Information on User IT Roles and Responsibilities
- Adapt to Changes with the Enterprise
  - System of Records/Fields
  - Approval Flows
  - Compliances

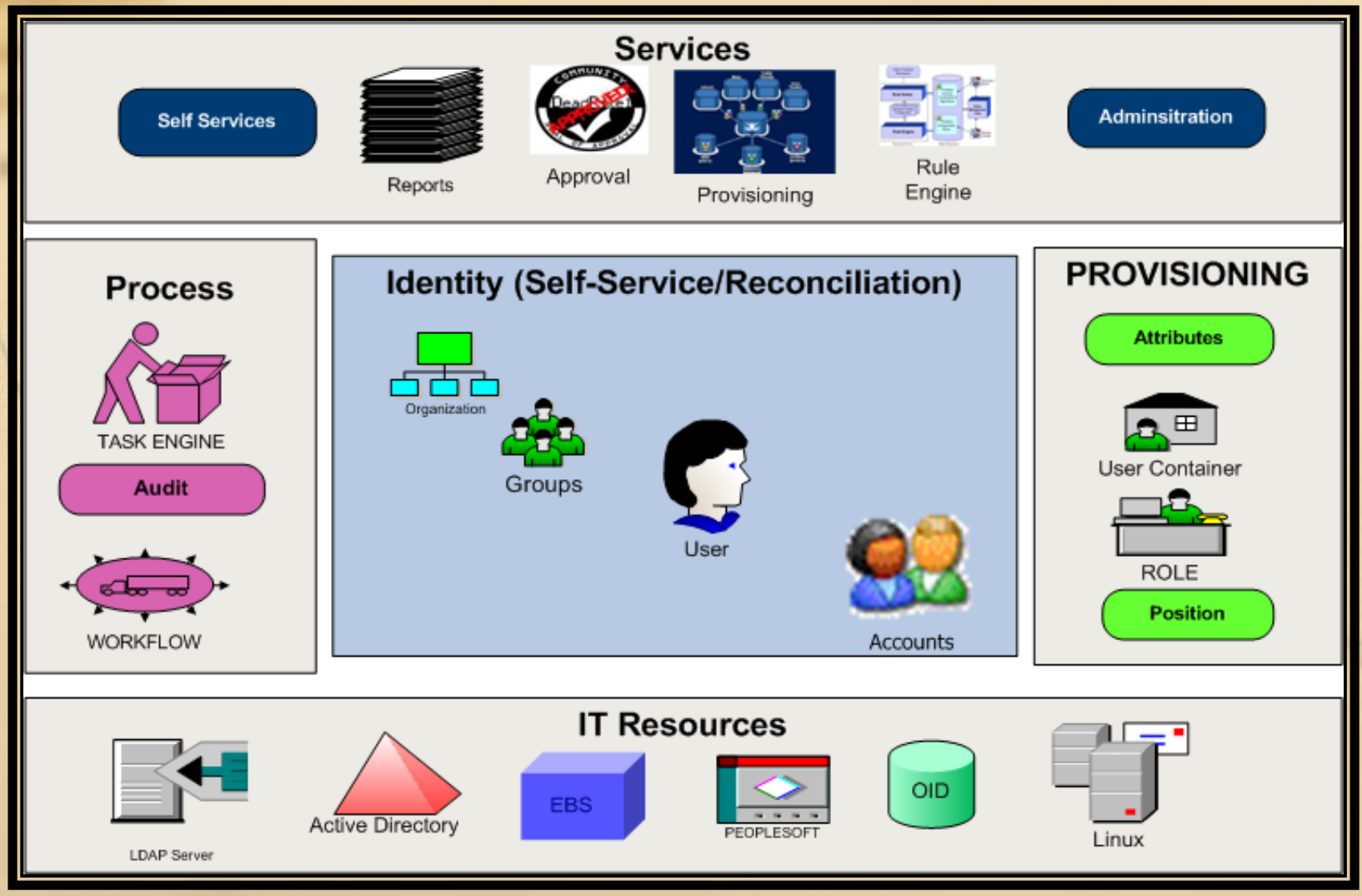
Modelling IM: Identity-Persona-Roles

IM – Technical Challenges

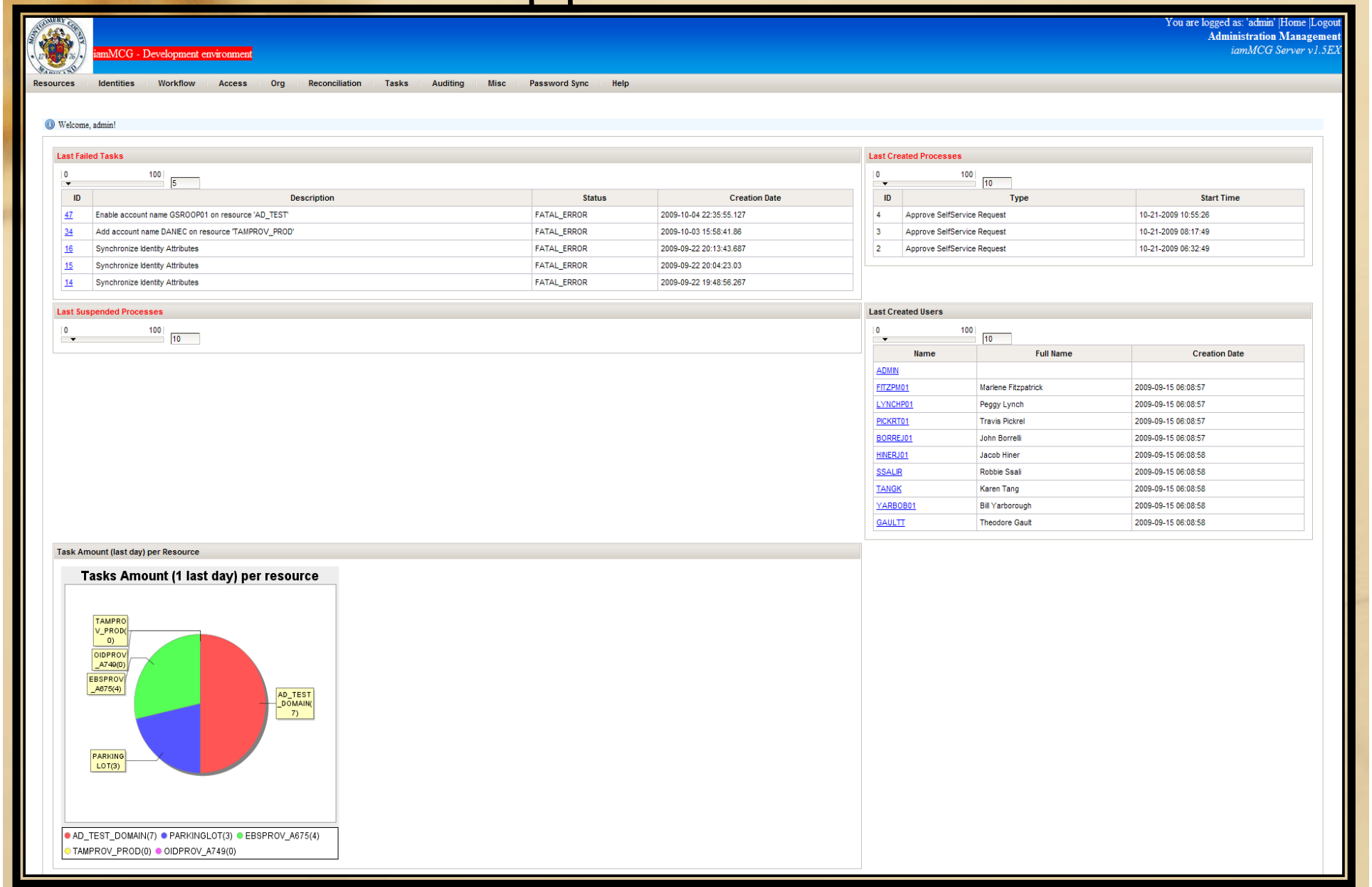
- IT Resources (Active Directory / EBS/ PSFT / RCParking) have their own User Account Management
- IT Resource Accounts Need Different Properties/Attributes
  - Logon ID, Unique Key ID, Email ID, Name and Location
- User Ends up with Multiple Accounts
- Enterprise Ends up Controlling/Managing/Transforming Multiple Accounts

An Enterprise Identity Links All Accounts to Represent the Single Person – iamMCG!

iamMCG Application Architecture



iamMCG Application



iamMCG Features - Functional

- Consolidated Employee Identity Attributes repository
- User and Access Reconciliations
- Integrated work-flow engine for complex business processes
- Provision Access and Permissions to All Resources
- Self Service interfaces
- Supports Complete Account Operations
- Centralized Password Policy and Password Synchronization.
- Policy Enforcements, Auditing & Compliance.
- Advanced Report Designer & Web-based Reporting Manager.

iamMCG Features - Technical

- Robust Provisioning Services
  - Tasks, Task Queues, Schedulers, BPM
- Supports many IT Resources (EBS, AD, TAM, PSFT)
- Role Based Access Control (RBAC)
- SPML V2 compliance.
- Rich Identity Model and Processes
- Accounts Attribute Synchronization
- Powerful scripting support for complex processes via Scripting expressions (20 different scripting languages!)
- Remote services access via Web-Services.
- Extensible via Events.
- Pluggable Authentication Handlers.
- Runs on any J2EE server; any Database Server

iamMCG Functional Differentiators

OIM	iamMCG
User, Group Objects and Attributes Only	Users, Groups, Orgs, Roles, Positions
Roles are through Groups (or buy ORM!)	Roles are First Class Objects
'Flat' representation of Identity	'Hierarchical' Representation to Match Organization: Positions with Roles Roles with Inherited Roles User can have Many Positions/Roles
Provisioning by Identity Attributes	Provisioning by **Roles and Positions**
Predefined Reports	Open Standard Reporting Engine
Self-Service for User Accounts	Self-Service Possible to Delegate All Functions (Approval Flow for Accountability)
Implements Standard Identity Processes	Implements Additional Advancements Delegate Roles Temporarily Clone Accounts Resource Reconciliations

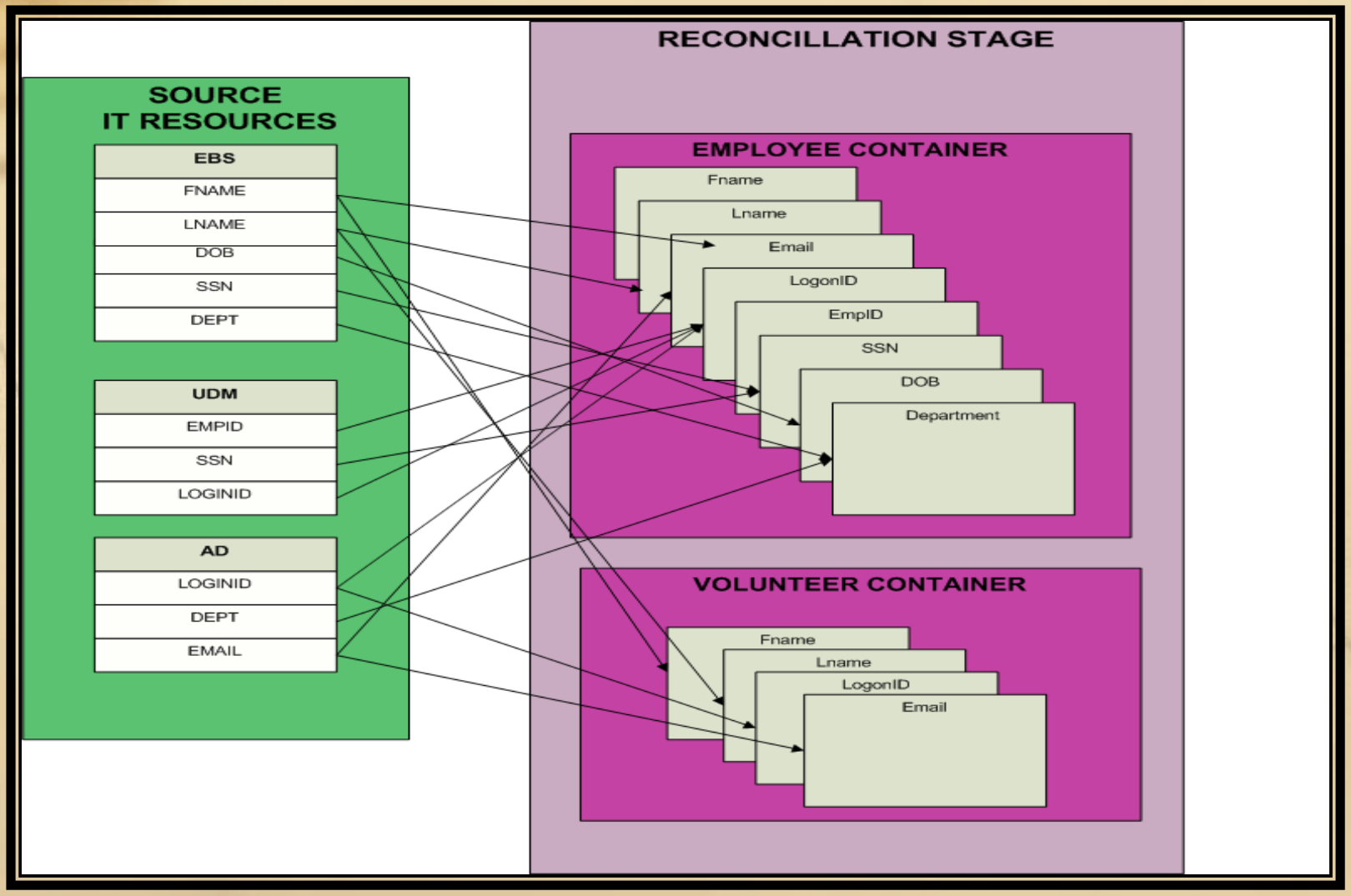
iamMCG Technical Differentiators

OIM	iamMCG
Custom Workflow	Standard BPEL Workflow
Custom Rule Engine	Standard J2EE Rule Engines
Custom Design Patterns (Skill Set)	Inversion of Control (Injections) Seam flow configuration Script Engines Standard Report Engine (Eclipse BRIT)
Predefined UI Screens	Seam Injection of 'portlets'
Custom Architecture	Industry Standards Based SPMLv2 BPEL (jBPM) Seam Security Models (SSL, JAAS) Java EE 5
Lots of Predefined Connectors ($$$)	Connectors for Standard Resources (and TAM)
Licensed by Identity Count	Open Source

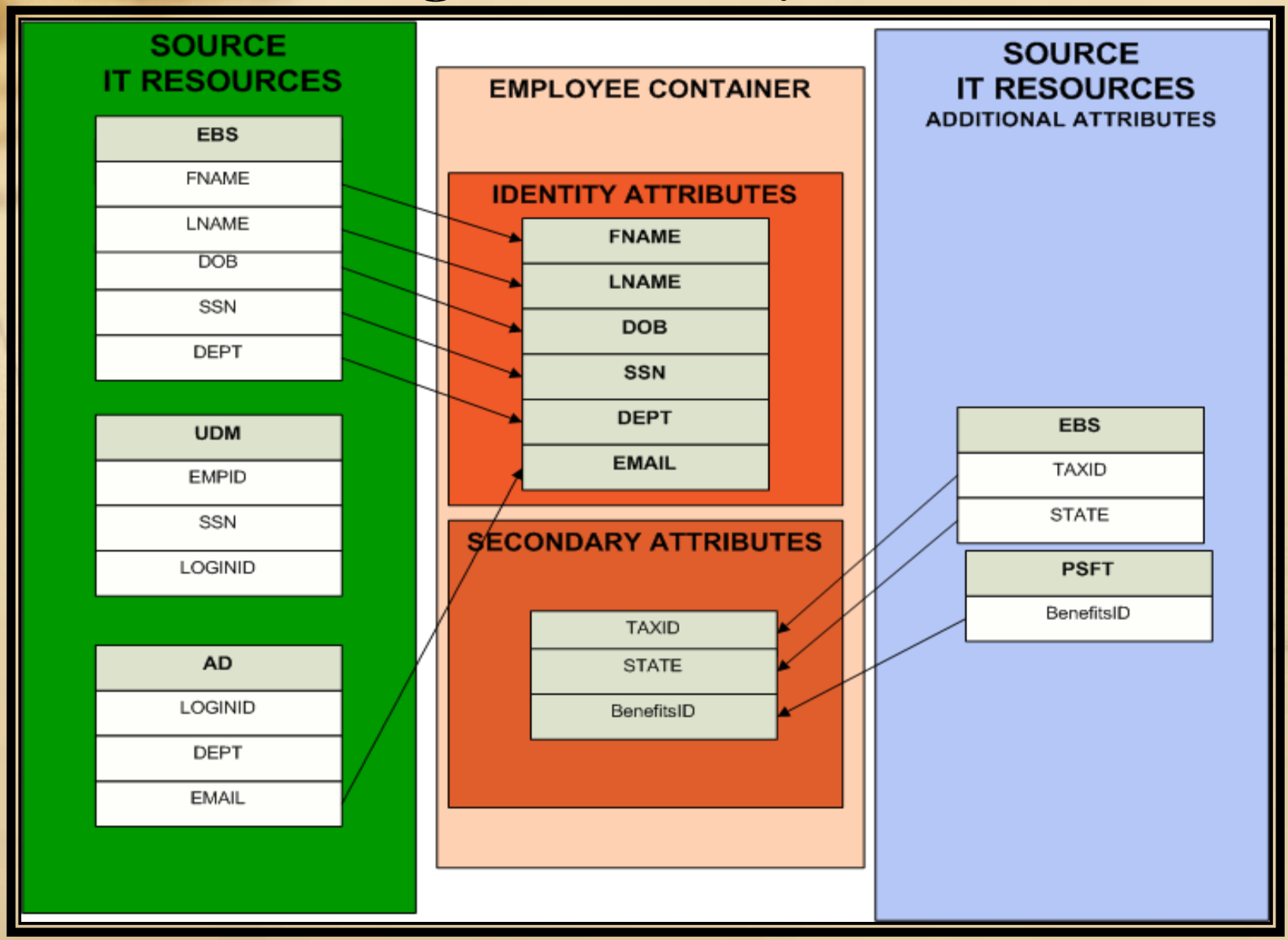
User Reconciliation

- Ability to Centralize User Properties/Attributes from Multiple System of Records
- Recon Could be One-time Activity – as Conversion to new System of Records
- Recon Could be Scheduled Activity for Ongoing System of Records
- Source of System of Records could Change with Enterprise
- Business Could Continue with Existing Process over System of Records
  - Change Address, Department Transfers, SSN/Employee ID
- Examples
  - Active Directory (Email, SSO Logon, SSO Password)
  - UDM (EmployeeID, SSN) – Temporary System of Records
  - EBS-HRMS (Name, SSN, Address, Department)

iamMCG – User Reconciliation



Reconciling Secondary Attributes



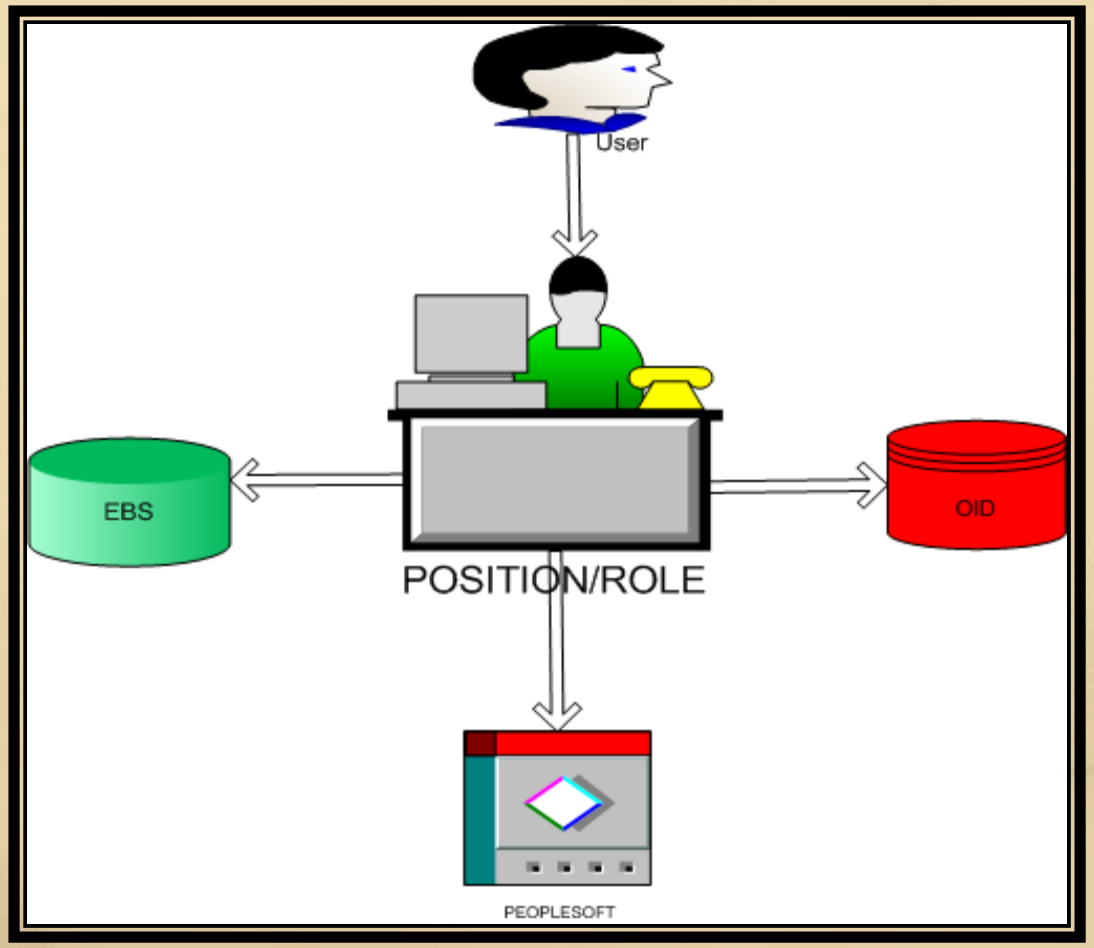
Resource Reconciliation

- Ability to Enforce iamMCG as System of Records
- Accounts in iamMCG will be Verified for Role Permissions
- New Accounts in iamMCG will be 'Provisioned'
- Accounts NOT in imaMCG will be Disabled
- User Records Include Resource Accounts Records (Available for Review)
- Real-time Reports on Current Roles and Permissions over Resources
- Ability to Control User Attributes/Properties Sent to Resources
- IM Standard Implementation (SPMLv2)

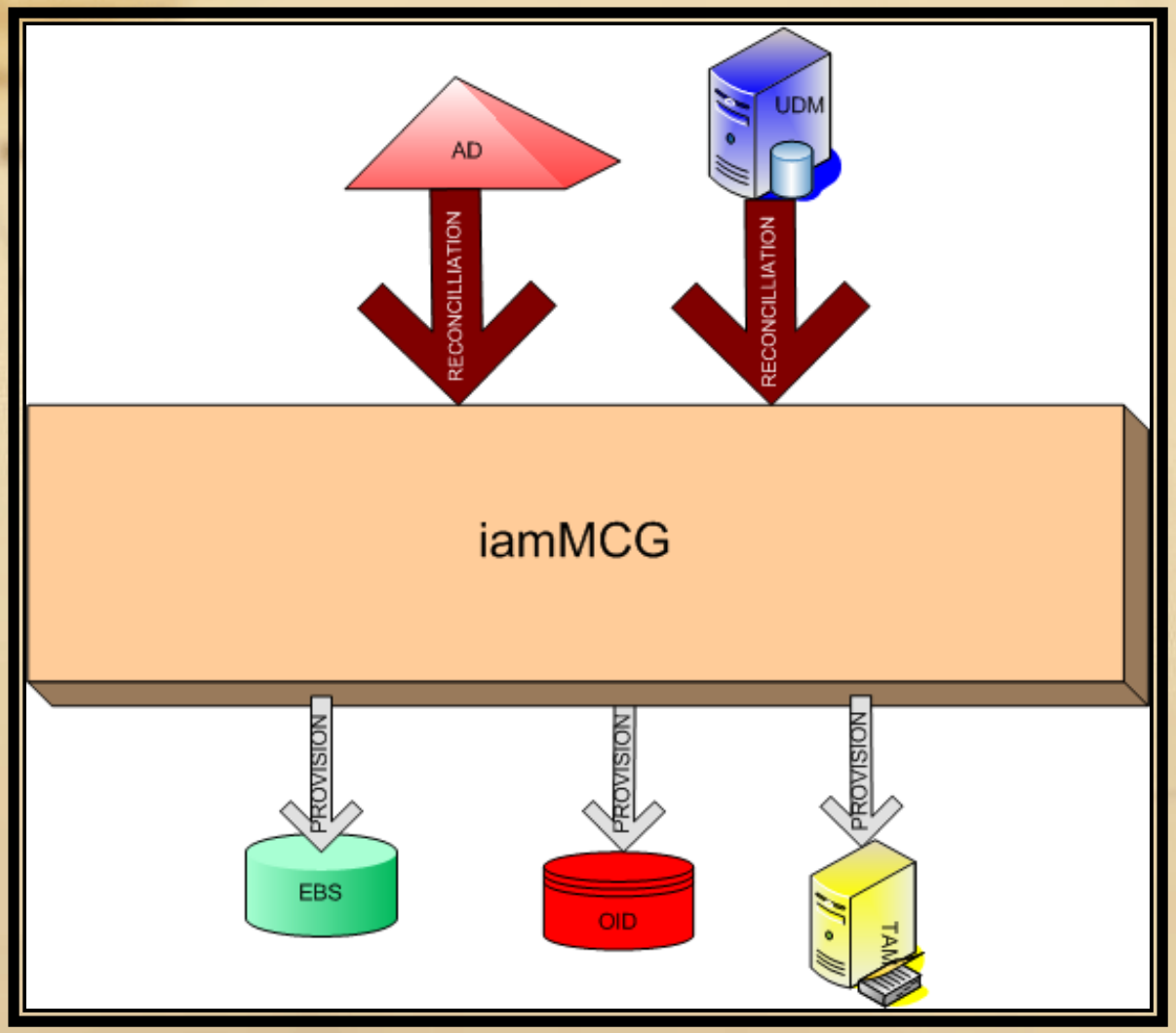
Provisioning/Deprovisioning

- Creation, maintenance and deactivation of Accounts with Attributes for IT Resources
- Done in Response to Automated or Interactive Business Processes.
- Users may be Represented by Multiple Accounts on Multiple Systems.
- iamMCG User Provisioning/Deprovisioning Service Include Following Processes:
  1. Role/Position based Provisioning
  2. Change Propagation
  3. Self Service Workflow
  4. Consolidated User Administration
  5. Delegated User Administration
  6. Federated Change Control.
- User of Various Types (employees, contractors, vendors, partners, customers) can get different Position/Role packs.
- Examples: EBS Access Permissions, Report Access, Email, Inclusion in a published user directory, Access to a Database, Access to a Network or Mainframe

iamMCG – Provisioning/Deprovisioning

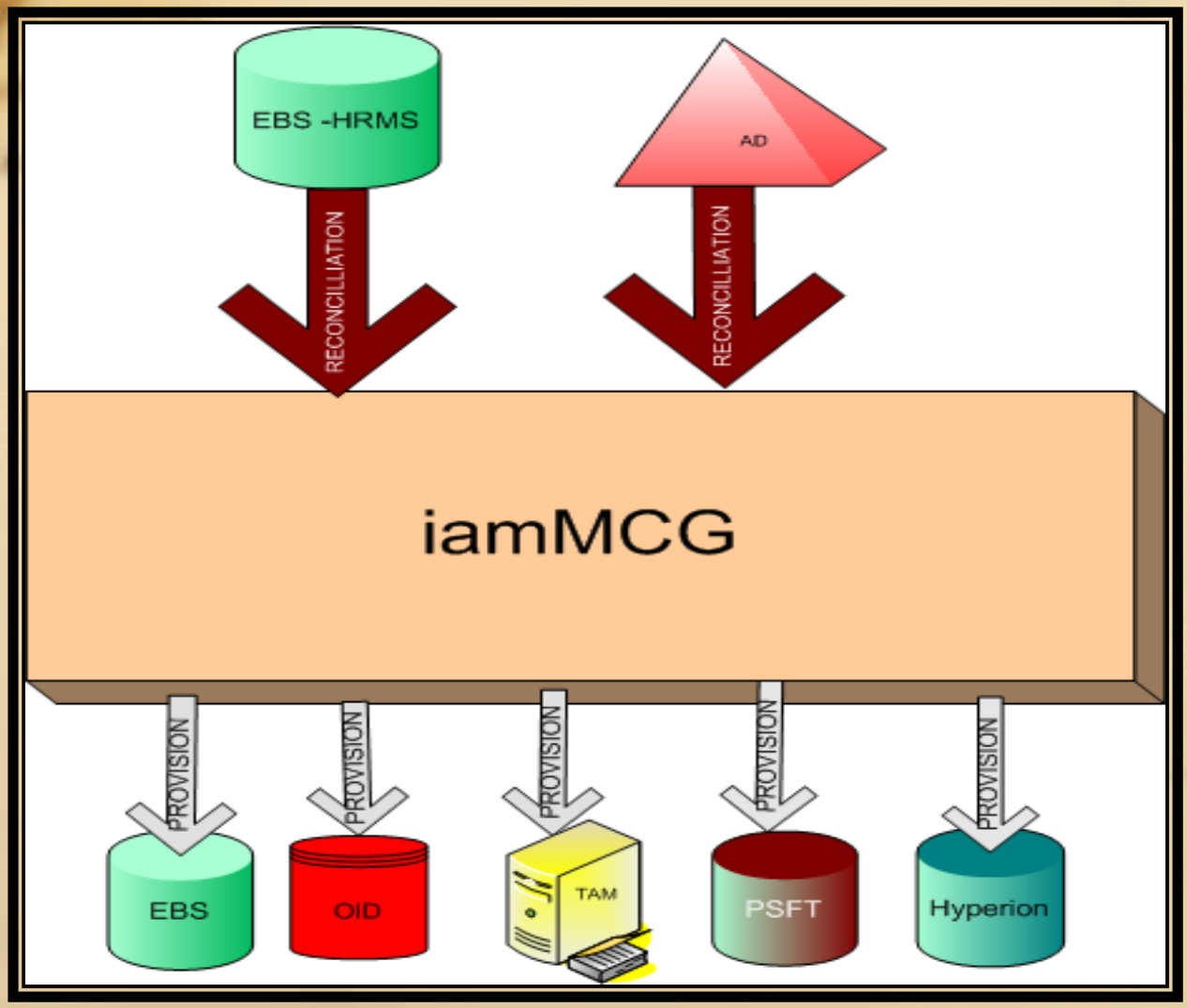


Evolve iamMCG – Initial Version



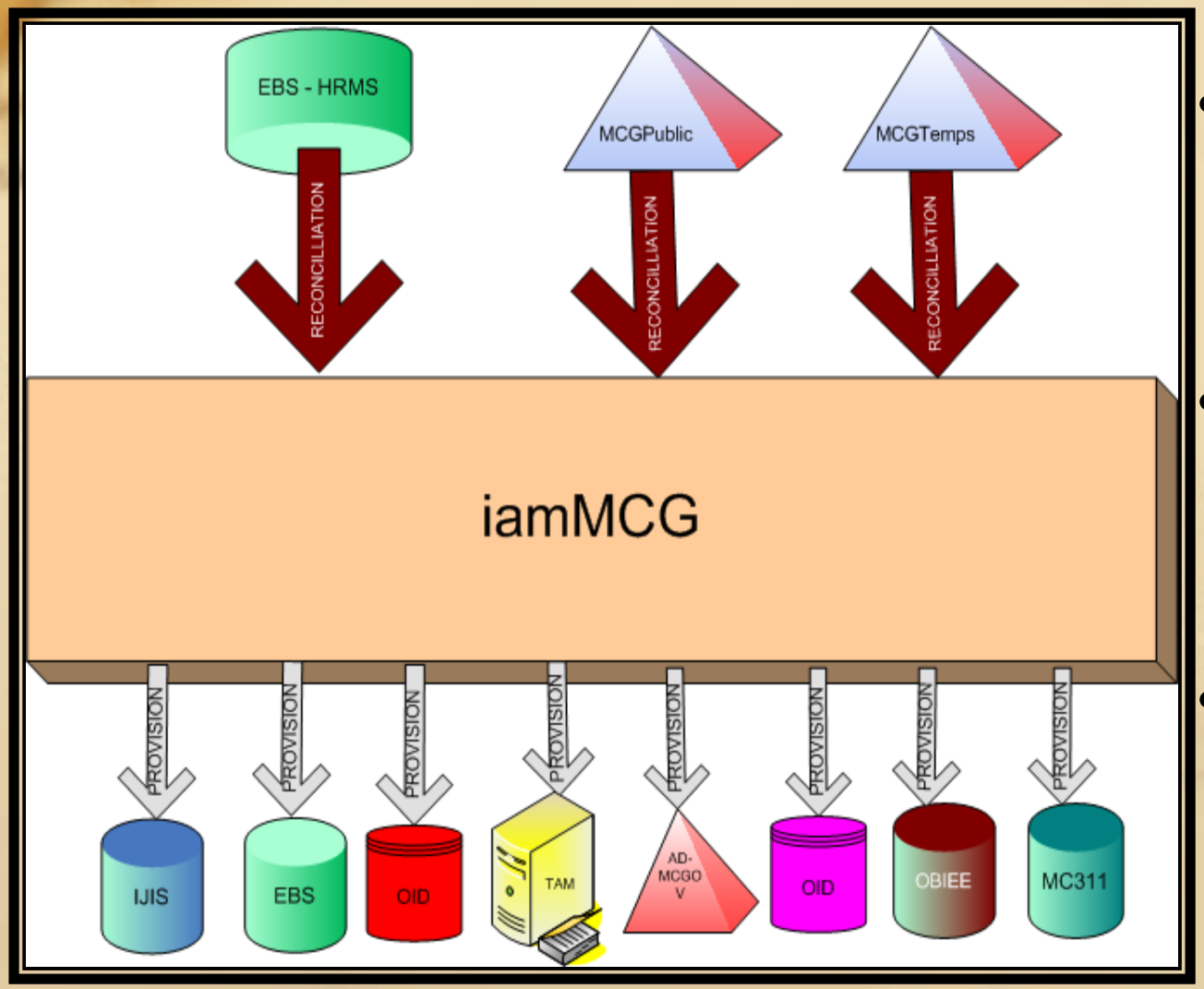
- Start with Current Realities!
- Utilize Core Competencies
- No Business Process Changes!

Evolve iamMCG – EBS-centric



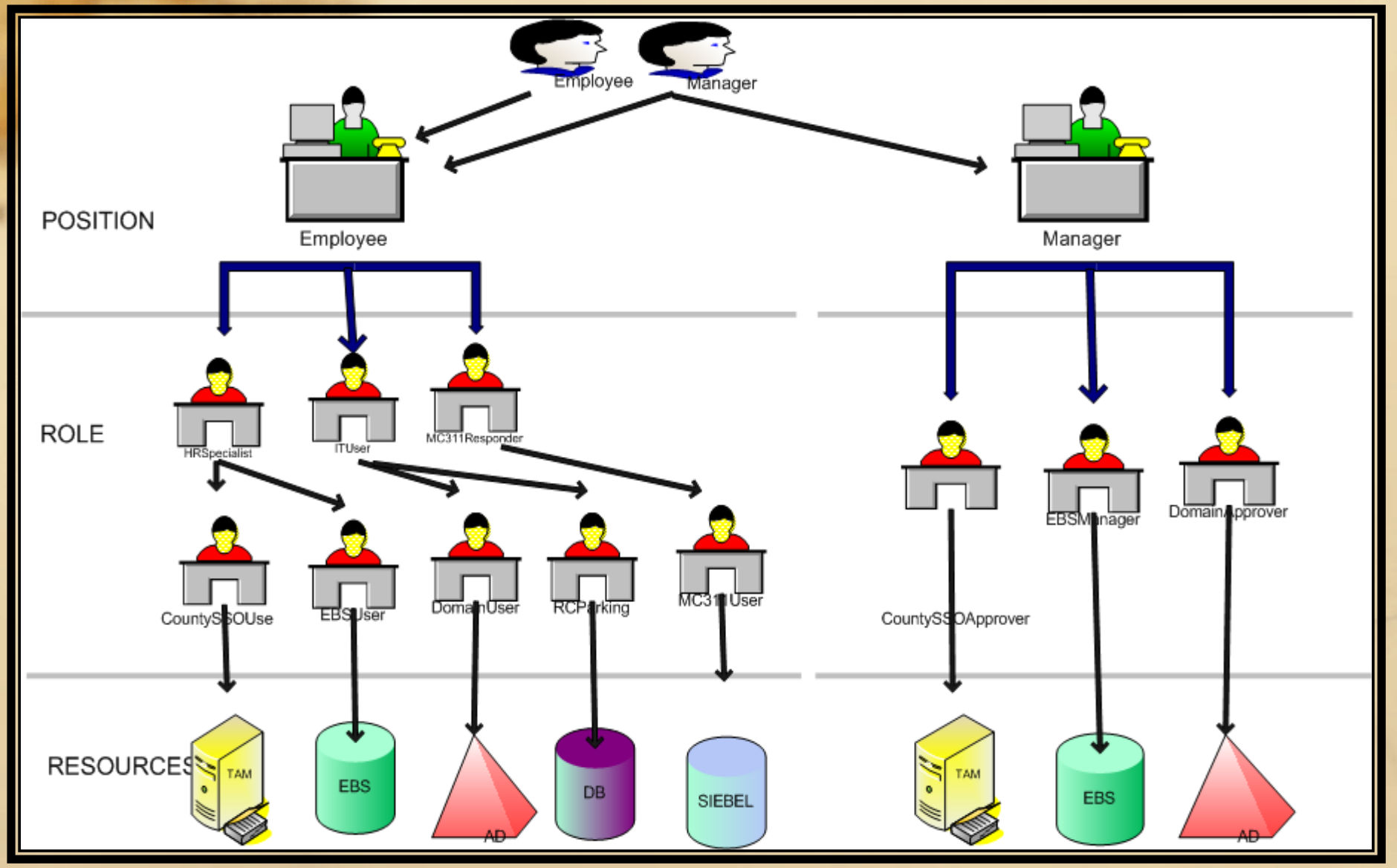
- Transform to ERP-centric Processes
- Forge to Single System of Records!
- Define AD Provisioning Processes

Evolve iamMCG – Federated

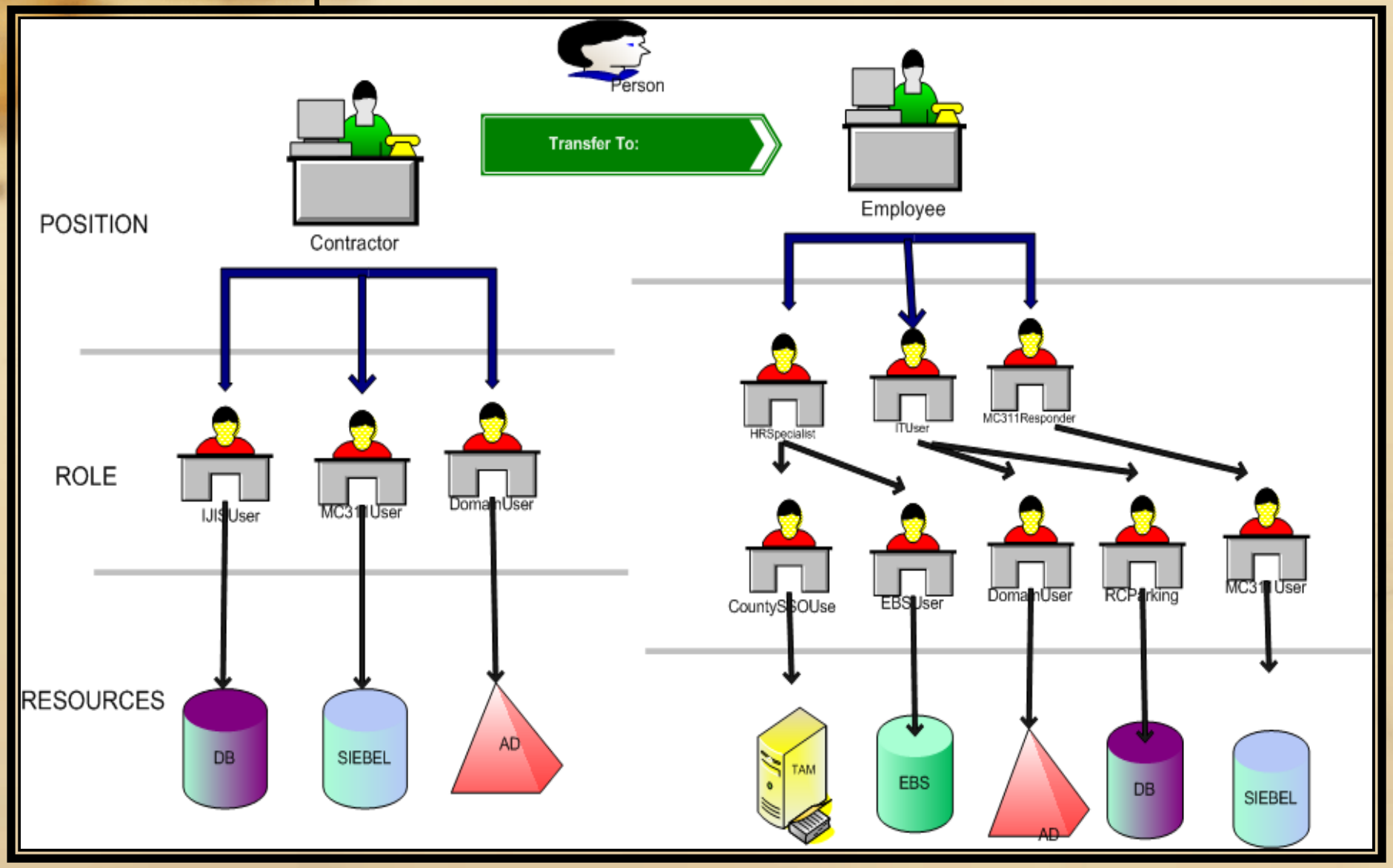


- Identity For County Participants!
- Multiple Sources of Identities
- Single Source of IT Access Controls!

Persons/Positions/Roles/Access!



Temp-To-Perm Transfer Scenario



iamMCG -- Self-Service

- Automated Provisioning
- Approval Workflow
- ‘Clone’ Identity (Identity Replacement)
- Temporary Delegate of the Roles
- Notifications
- Audit Controls

iamMCG – Current Status

- **In Middle of Federated Version**
  - MCG Public Extranet ~ 2500 Accounts
- **Implemented Full Reconciliations**
  - County Active Directory ~ 17000 Accounts
  - Oracle EBS Person Records ~ 23000 Accounts
- **Implemented Incremental Reconciliations**
  - CDC Change Data Capture; Near-Real-time Updates
- **Implemented Identity Attribute Reconciliations**
  - Single Representation of Truth

iamMCG – Current Status

- Implemented Roles Provisioning/Deprovisioning
  - Oracle EBS (User Creation, Responsibility Assoc)
  - Hyperion (User Creation, Group Assoc)
  - OBIEE (User Assoc, Group Assoc)
  - Tivoli Access Manager (County SSO)
  - 7 Other Apps
- Implemented Most of Core Functions
  - Self-Services for Resource Provisioning
  - Role Expiration/Deprovisioning
  - Journaling
  - Workflows
  - Reports

iamMCG – Next Steps (Functional)

- Replace UDM
- Implement Applicant-to-Employee Business Process
- Provision Users to EBS, Active Directory
- Identify Reporting/Auditing Requirements

iamMCG – Next Steps (Technical)

- ~~Complete Validation of ERP Resource Provisioning/Deprovisioning~~
- ~~Complete Validation of Infrastructure Resource Reconciliation, Provisioning/Deprovisioning~~
- ~~Deployment and Operational Support~~
- ~~Source Control/Documentations~~
- Performance Tunings
- DR

Demo!

- Activity Dashboard
- Identity Modeling
- IT Resource Modeling
- Role Modeling
- Identity Reconciliation
- Resource Provisioning
- Self Service for IT Access Provisioning

Ugh…


HELLO-WHO AM I?
AMNESIAC
ASSOC.
S LANE
searchID: csan34
© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com

Reference

- IM General Introduction
  - http://en.wikipedia.org/wiki/Identity_management
  - http://www.infoworld.com/article/05/10/07/41FEidm_1.html?s=feature
  - http://identityaccessmanagement.blogspot.com/2005/05/vendor-list.html
- IM Technical Introduction
  - https://identitymanagement.dev.java.net/
  - http://community.java.net/identitymanagement/
- Velo Website
  - http://velo.safehaus.org
- IM Architecture
  - http://wikis.sun.com/display/openptk/Project+OpenPTK