
ORACLE®

ORACLE OPEN WORLD

experience
OPENWORLD

November 11–15, 2007

ORACLE

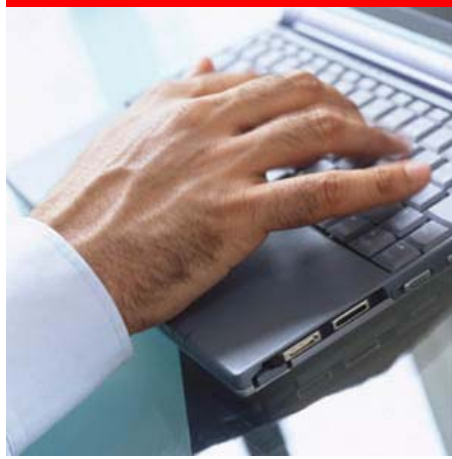
ORACLE

Rationalize, Centralize, Externalize: Identity Management in Oracle Fusion Architecture

Nishant Kaushik
Consulting Member of Technical Staff

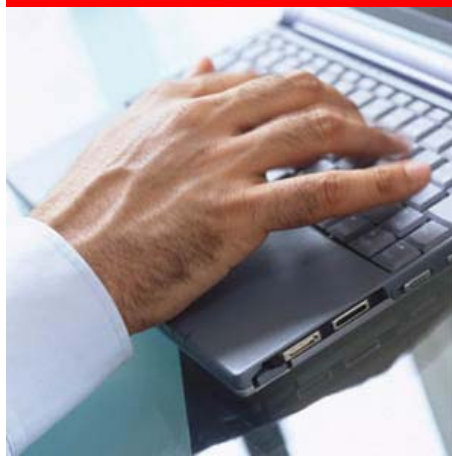
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.
The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Agenda



- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services

Agenda



- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services

Oracle’s Fusion Strategy

- Fusion Architecture
  - Blueprint for SOA-based Enterprise Solutions
  - http://www.oracle.com/applications/fusion.html
- Fusion Middleware
  - Technology Infrastructure for SOA Applications
- Fusion Applications
  - Unify best-of-business capabilities from all Oracle Applications in a complete suite delivered on Oracle's open technology
  - Protect, Extend, Evolve through Fusion Architecture

ORACLE FUSION

Security in Fusion

One Integrated Security Solution

- Rationalize, Centralize, and Externalize
  - Authentication policies / services
  - Authorization policies / decisions
  - User registration / provisioning / administration
- Built on Fusion Middleware
  - Enforced uniformly at all parts of technology infrastructure
  - IAM Suite will be basis for Identity Services
- Based on Standards
  - NIST RBAC
  - JAAS

Guiding Principles of Fusion Security

- Secure By Design
  - Security must be designed into the application, not added as an afterthought
  - Security is difficult & costly to add later
- Secure By Default
  - Restrict access out of the box
  - Many systems don’t get locked down
- Principle of Least Privilege
  - By default, no one should have access to anything
  - Users are explicitly granted access to the minimum set of resources they need, for the minimum set of time
  - Do not design application based on denies / negative grants

Our Challenges

- Each application collects its own user (identity) data during custom registration processes
  - No uniformity in data collection
  - No sharing of data
  - Multiple places for user to manage data
- Complex Authorization model
  - No role style abstraction models
  - Determining who has what privileges extremely complex
- Inconsistent Administration Experience
  - Difficult to enforce consistent set of policies
  - Difficult to measure compliance with those policies

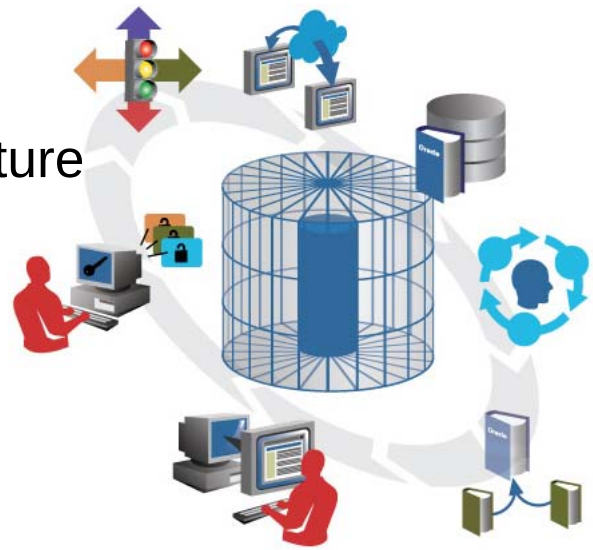
The Applications

- **Oracle eBusiness Suite**
  - Multiple user management modules (CRM user mgmt, UMX)
  - Role management limited to UMX
  - Directory integration requires OID + DIP
- **PeopleSoft**
  - No provisioning or role management support
  - Multiple integration interfaces
  - Component Interface, Integration Broker / Application Messaging
- **Siebel**
  - No provisioning or role management support, relies on 3rd party tools
  - No directory integration tools

How Identity Management Helps Today

Security And Control For Enterprise Applications

- Deploying Oracle IAM can help alleviate some of the issues for your applications deployment by:
  - Establishing an Enterprise Identity & Roles
  - Enforcing Strong And Granular Security Policies
  - Automating Security Related Processes
  - Defining an Audit And Control Framework
  - Deploying A Scalable Integration Architecture



How Identity Management Helps Today

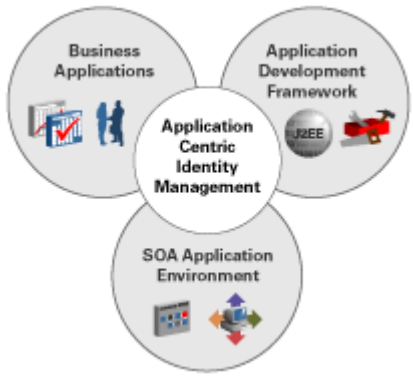
Security And Control For Enterprise Applications

- Enable SSO, federated access, mutual authentication and fraud prevention
- Automate user management, manage entitlements, enforce segregation of duties
- Link HR employee data and CRM customer data to user accounts
- Integrate application to enterprise directories and portals
- Enforce appropriate and granular level of access control based on application and data being accessed
- Automate compliance and fraud management
- Deploy self-service and self registration to reduce administration cost

But Where's The 2.0 Stuff?

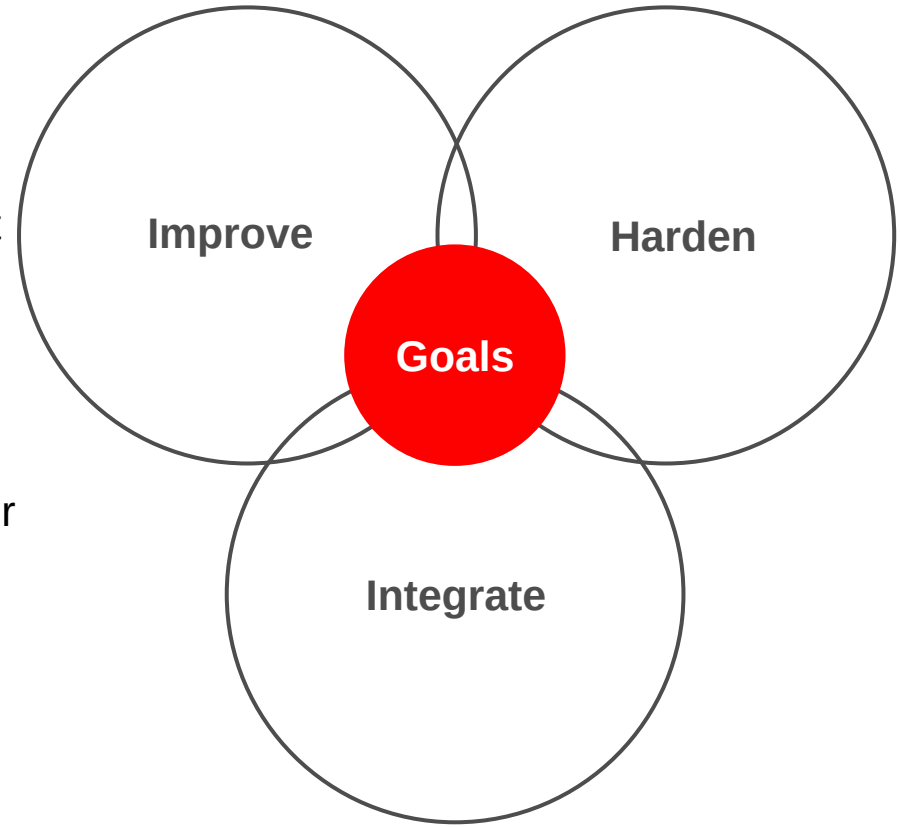
Last Year at OpenWorld

- S281669: Application-Centric Identity Management: Identity-enabled applications made easy
  - Introduced the concept of **Application-Centric Identity Management**
  - Talked about how identity is central of application design
  - Talked about evolving IdM from **System Management** tool to **Platform Infrastructure**



The Goals

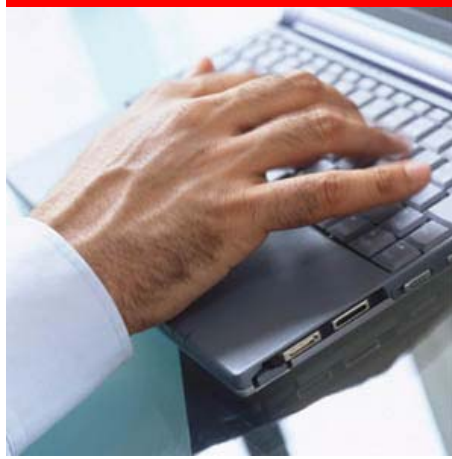
- Establish “One Human ↔ One Identity” for the entire deployment
- Simplify the administration experience
- Reduce cost
- Improve developer experience & productivity



- Reduce # of points of failure
- Reduce # of modules with potential for security holes
- Enforce security regardless of entry point
- Customers and Auditors must be able to setup, change, audit, and review security policies in a single place

- Integrated & understood across all components / tiers
- Single integration point to 3rd party solutions & future technologies

Agenda



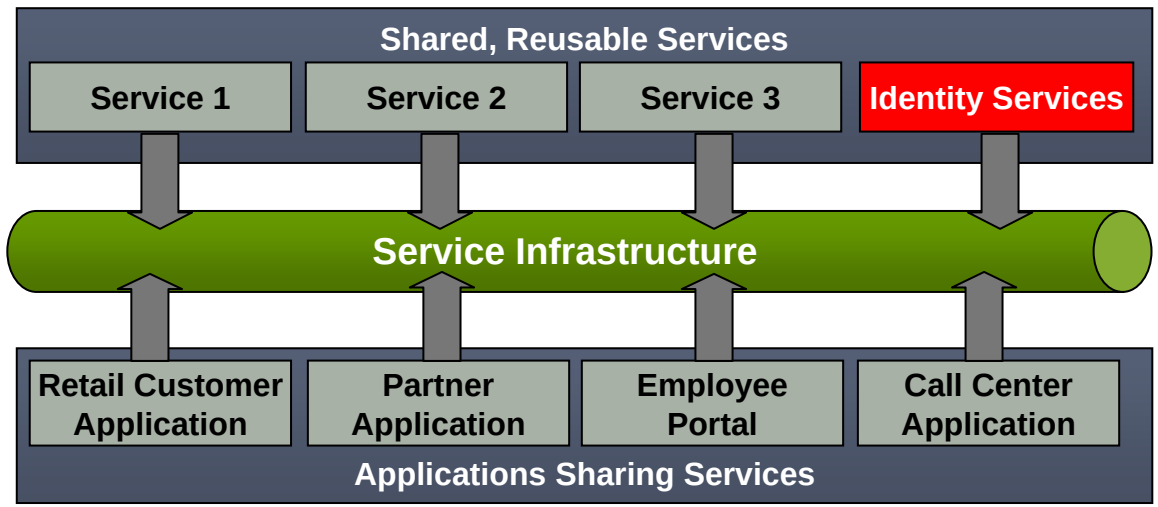
- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services

Identity Management in Fusion

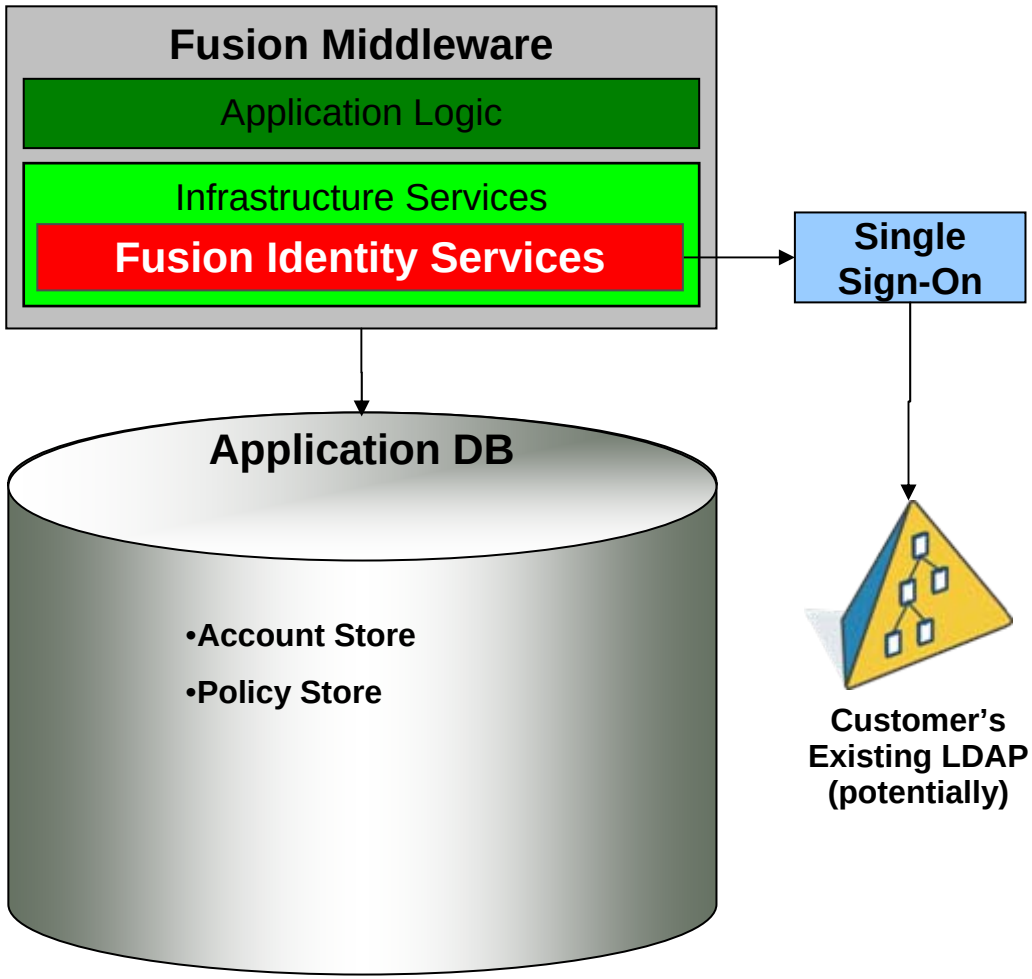
- Unified Identity Management services (both self-service and administrative) across all Oracle applications
- Complete and integrated lifecycle management with person (employee, partner, customer) on-boarding
  - Standards-based
  - J2EE, SAML, WS-*, …
- Superior Ownership Experience
  - Lower Cost Deployment, Operations, Compliance
- Unbreakable Security
  - RBAC model
  - GRC Framework

Builds on Vision of Identity Services

- As organizations move towards SOA, identity components and management capabilities must be made available as a service in that architecture



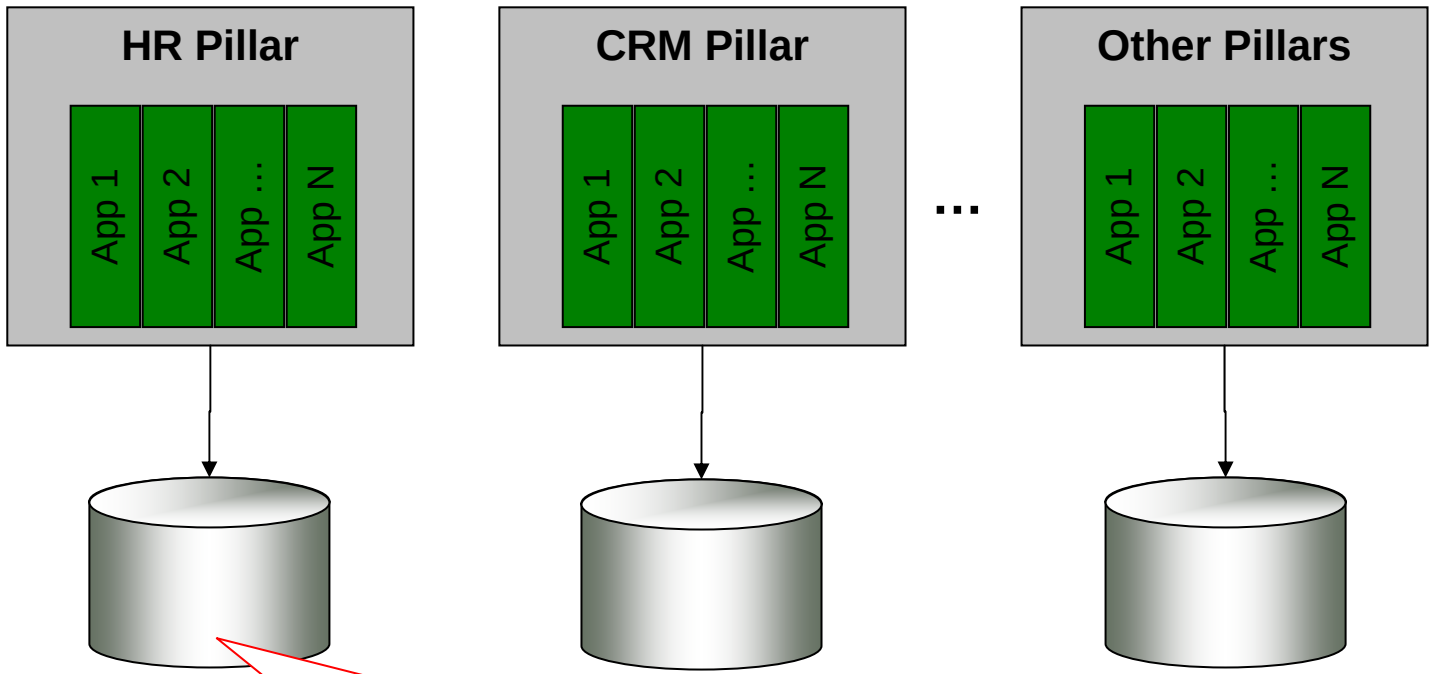
Fusion Application Architecture



Functional Architecture

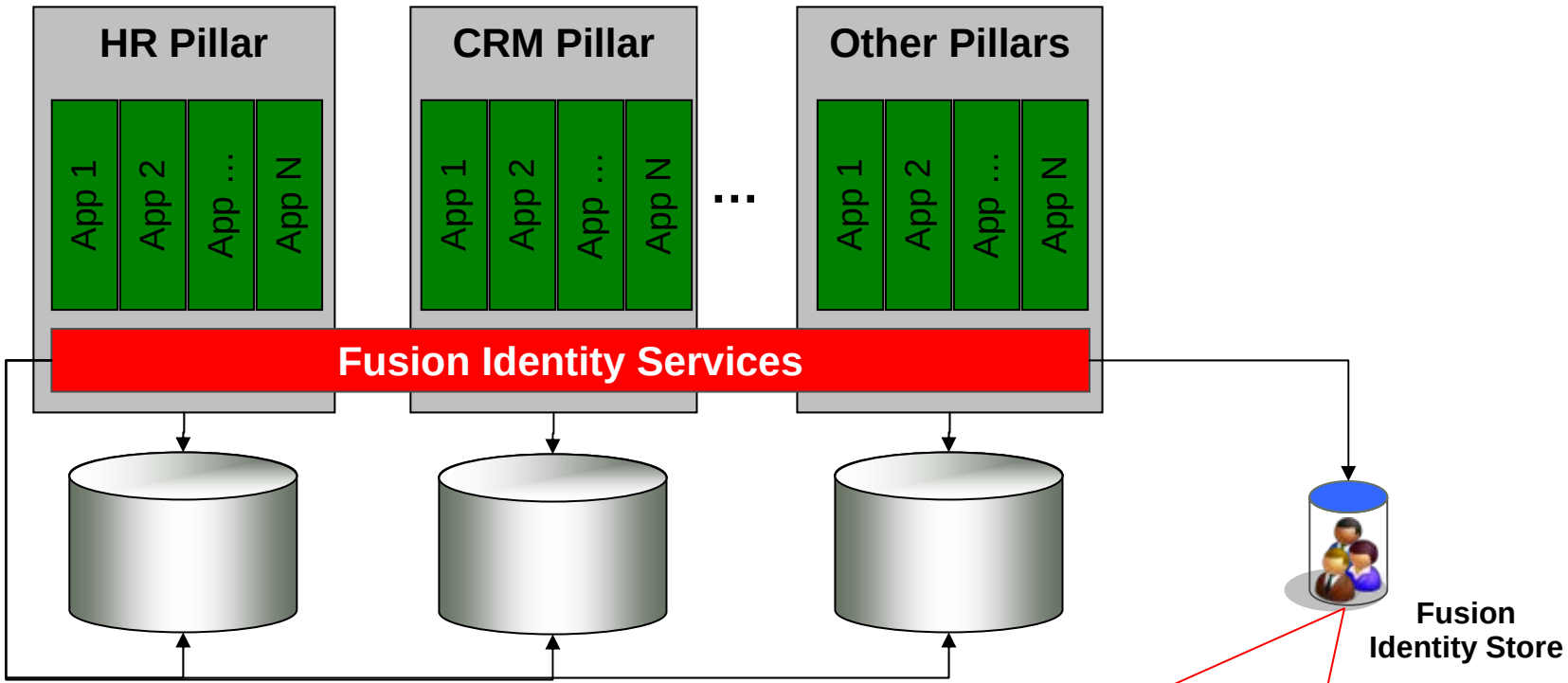
- An Identity has an "Account" in an application if it is represented in the LUS
- Account has privileges based on Roles assigned to it
- XS Policy Store maps the Roles to Privileges (Function, Data) in the Application
- XS Decision Point in DB ensures consistency in security no matter how user is connecting (through App or directly to DB)
- Authentication is managed via a Single Sign-On product (Oracle or Customer's existing)
- For existing SSO deployment, an LDAP system may exist as SSO credential store
- Foundation Identity Data stores identity data in Fusion data tables for fast transactional computations

Pillar Deployment



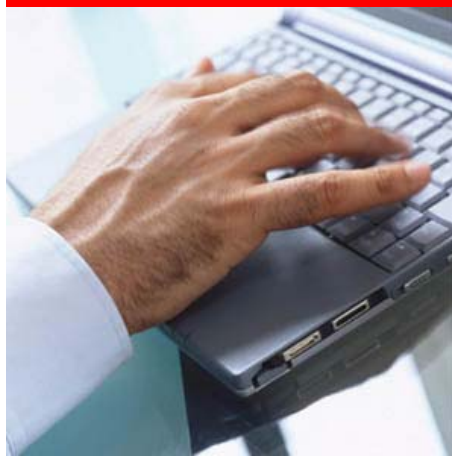
- Having entry in a particular Account Store means “having” an account in all applications in the pillar (access rights depends on roles assigned)
- In a Global Single Instance (GSI) deployment, all the pillars share a single DB (and therefore single Account Store)

Identity Management in Fusion



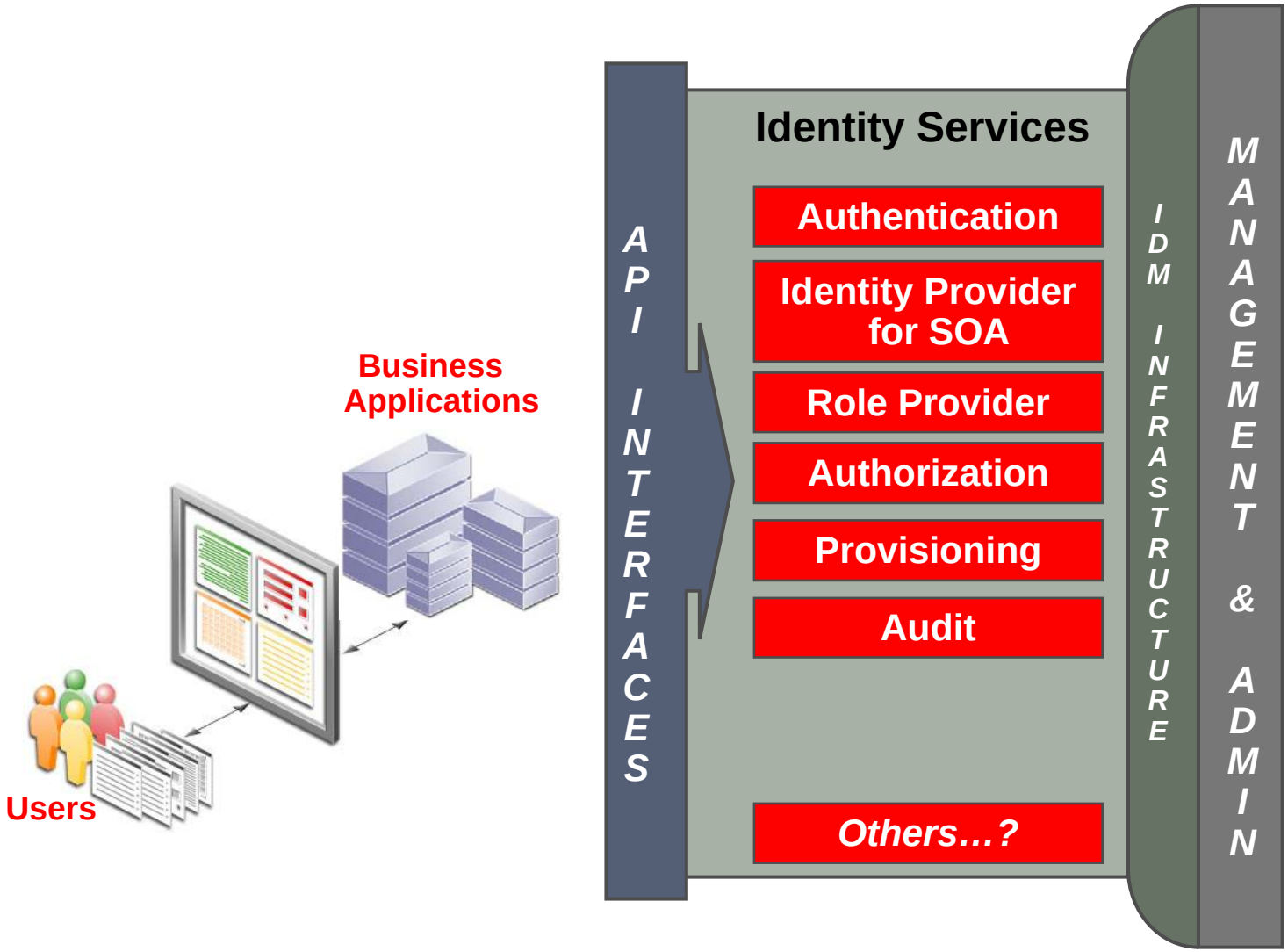
- Implements a single view of identities across entire Fusion deployment
- Either a Physical Store or a Virtualized Store depending on nature of deployment

Agenda

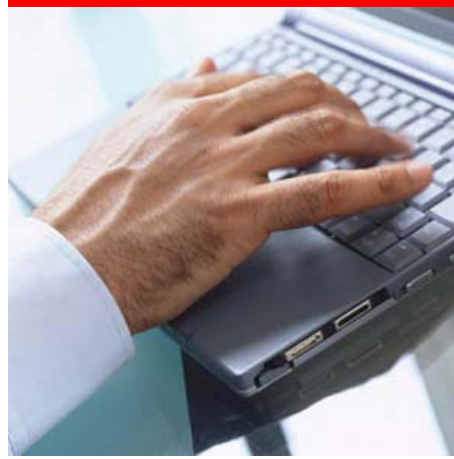


- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services

The Identity Services Layer



Agenda



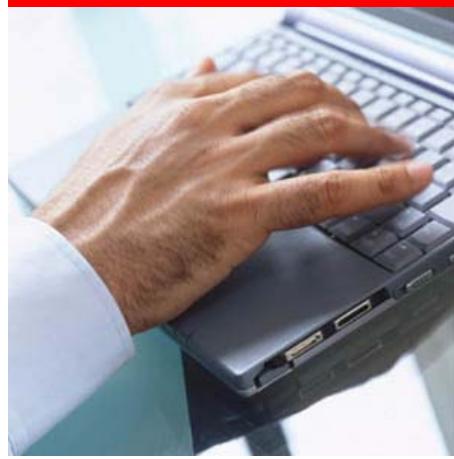
- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services
  - Authentication Service
  - Identity Provider for SOA
  - Role Provider
  - Authorization Service
  - Provisioning

Authentication Service

Externalize User Identification

- Authentication Service provides the right level of assurance to the application regarding the identity of the interacting user
- Integrate with existing SSO infrastructure via a plug-in model
- Support risk-based identity assurance levels
  - Beyond username-password
  - Beyond binary authenticated/unauthenticated
- Mutual Authentication
- Evolve for the future
  - User-Centric Technologies (CardSpace, OpenID)
  - Multi-Token authentication support

Agenda



- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services
  - Authentication Service
  - Identity Provider for SOA
  - Role Provider
  - Authorization Service
  - Provisioning

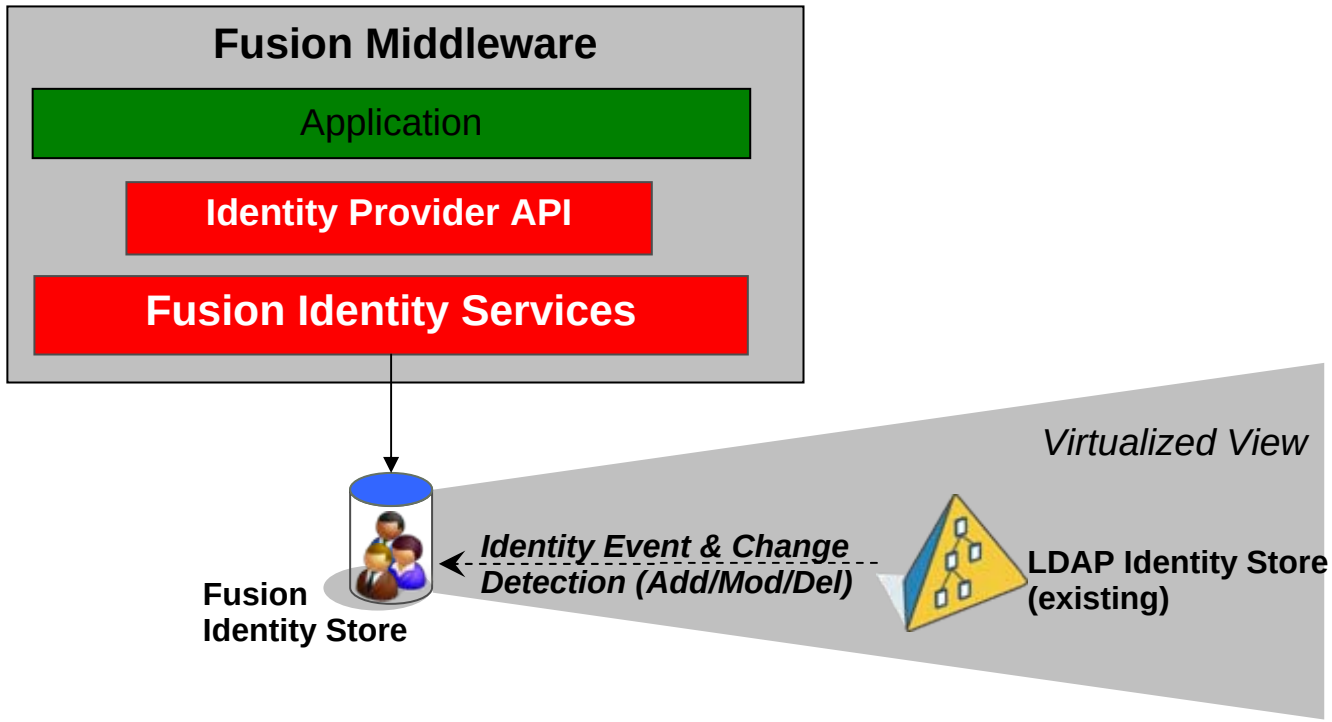
Identity Provider for SOA

Externalize Identity Data

- Identity Service that provides access to Identity Data
- The Goal: Get away from User tables that store identity information
- Support multiple sources of Identity Data in the Enterprise
  - HR, CRM, Custom Databases/Directories
- Create complete identity profile across
  - Identity Applications, Identity Stores, Cloud Identity Providers, User-Centric Identity
- Provide developer friendly API
  - Avoid application developers having to learn and code to LDAP
  - Support rich identity data

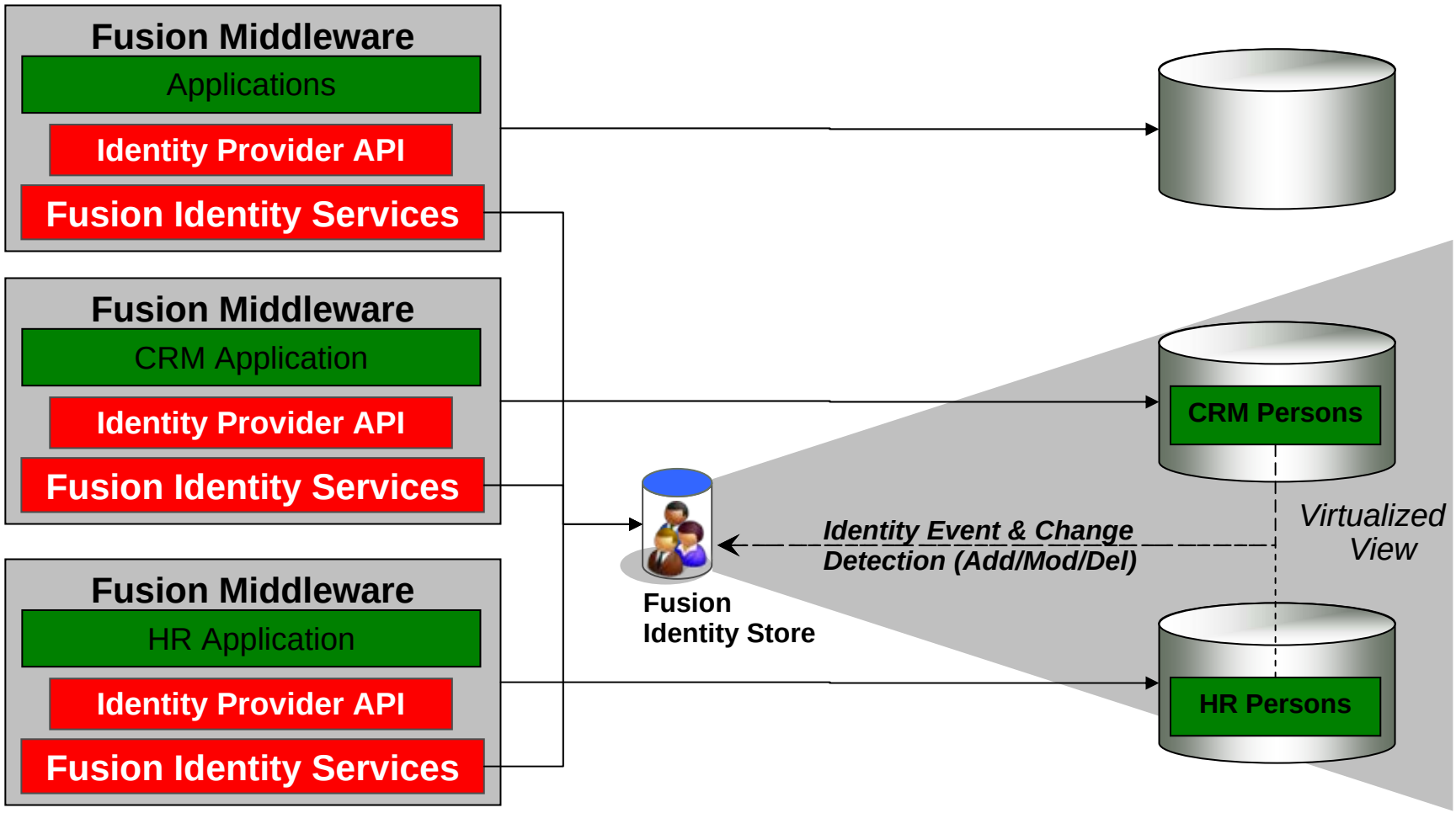
Identity Provider for SOA

Virtualized LDAP Identity Store

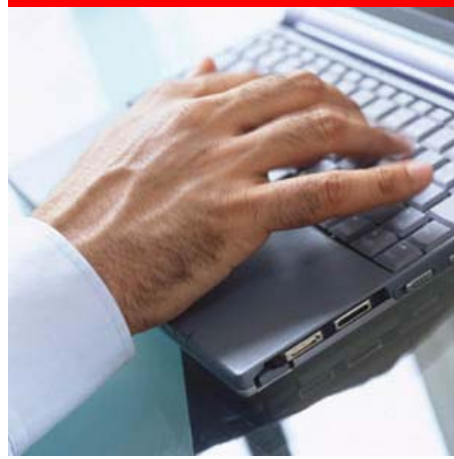


Identity Provider for SOA

Virtualized HR, CRM Identity Store



Agenda



- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services
  - Authentication Service
  - Identity Provider for SOA
  - Role Provider
  - Authorization Service
  - Provisioning

Role Provider

Centralize Role Management

- Service that provides information on roles and role memberships
  - Roles are necessary abstraction to make management of users manageable
- Fusion Security is based on NIST RBAC standard
  - ANSI INCITS 359-2004
  - Authorization policies built on role membership
    - Function Security
    - Data Security
  - One-To-Many Relationships
    - User can be assigned several roles
    - Role can be assigned to several users

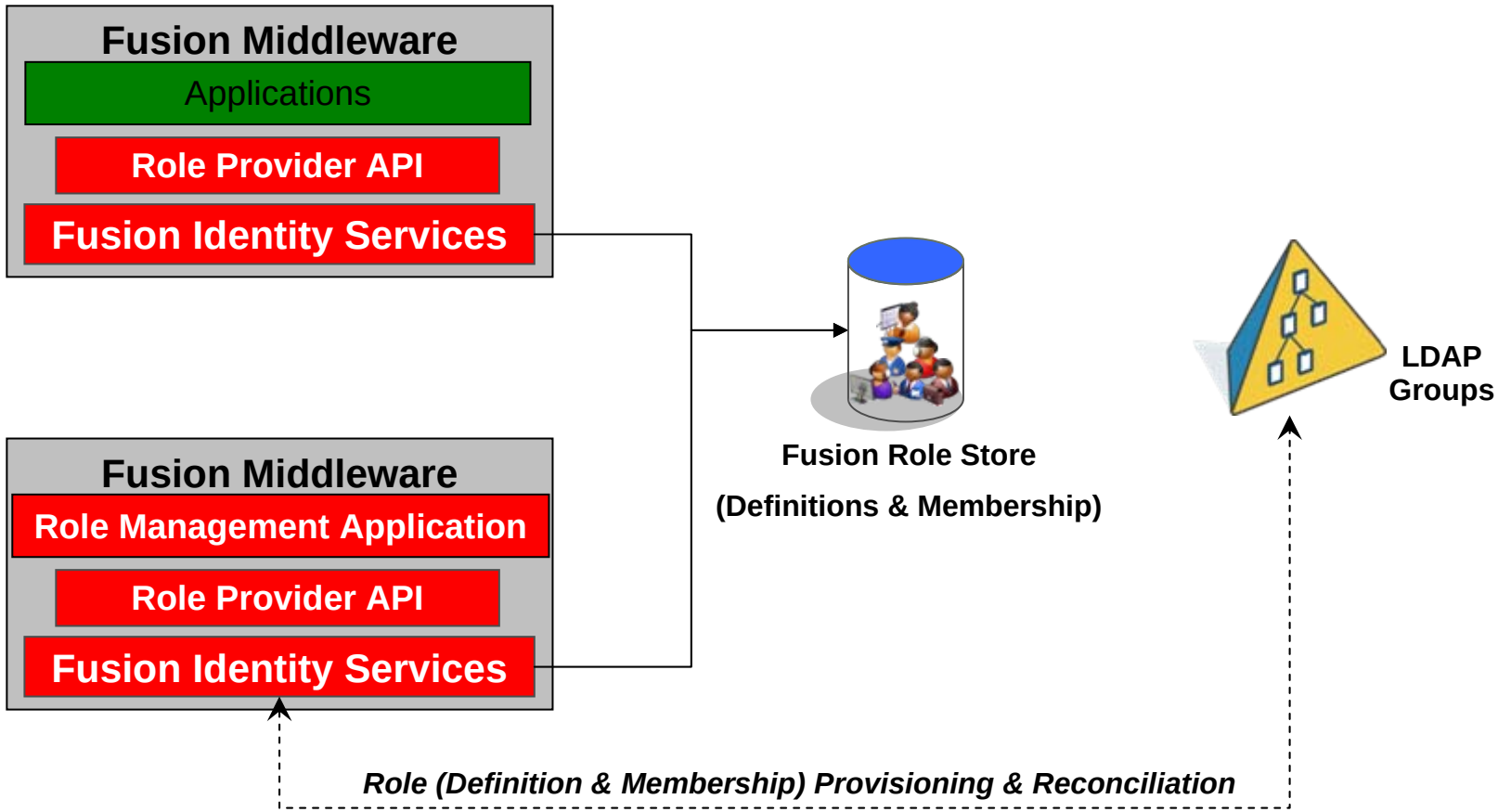
Role Provider

Centralize Role Management

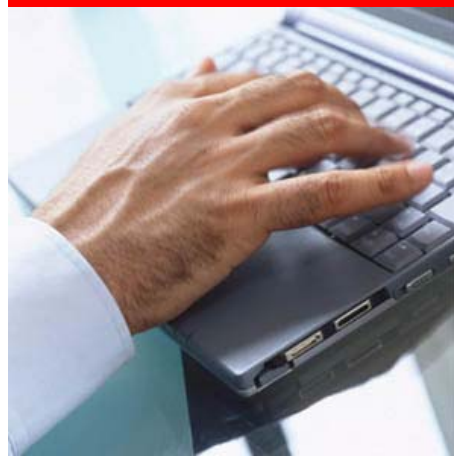
- Role Definition Management
  - Role Definition, including types, tags, catalogs and other attributes
  - Support effective dates
  - Role Inheritance Hierarchies
  - Enterprise and Application Roles
  - Import LDAP Groups as Enterprise Roles
- Role Membership management
- Role Controls
  - Membership approval
  - Membership rules
  - SoD Policies
- Automatic Role Assignment based on Policies

Role Provider

Centralize Role Management



Agenda



- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services
  - Authentication Service
  - Identity Provider for SOA
  - Role Provider
  - Authorization Service
  - Provisioning

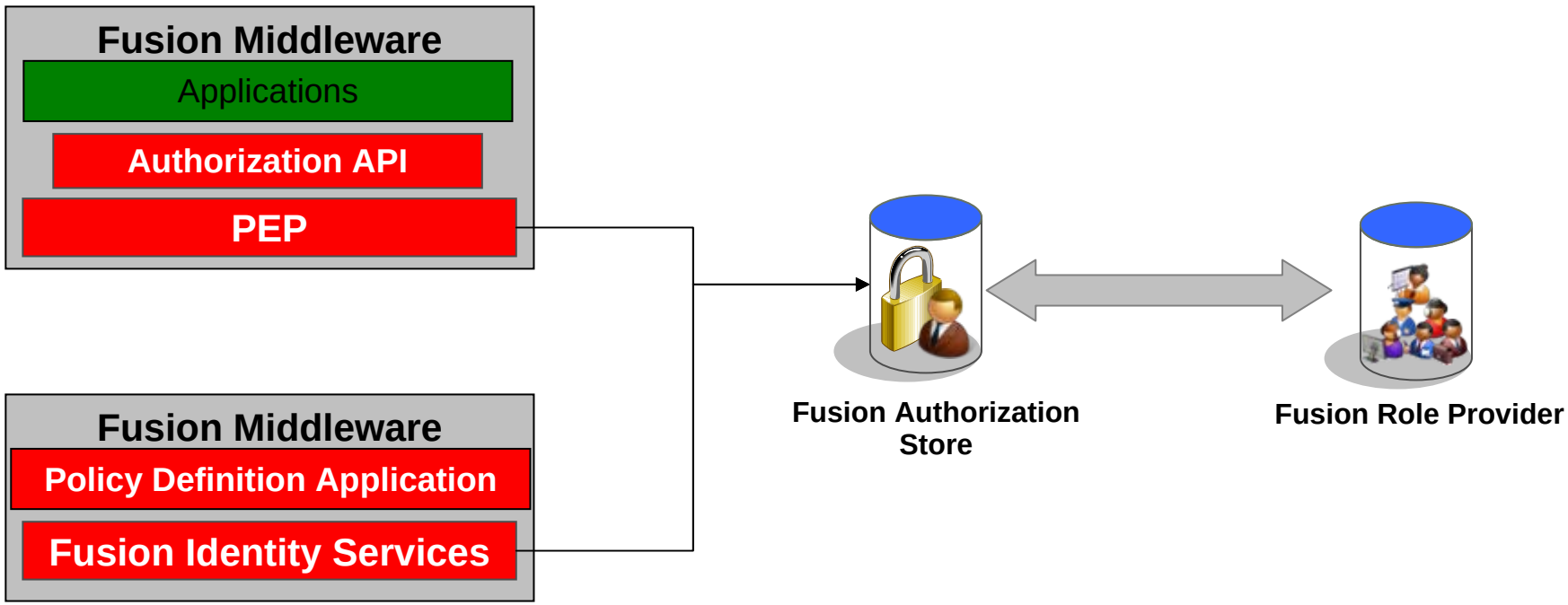
Authorization Service

Externalize, Centralize Authorization Policies

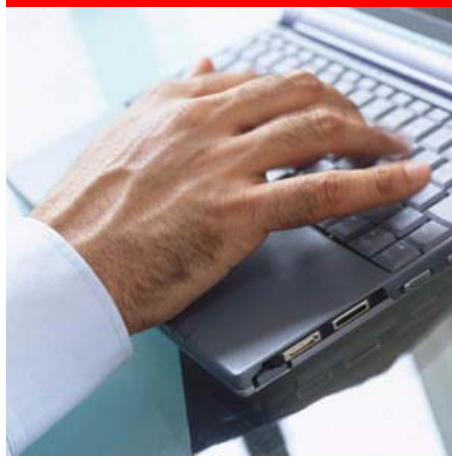
- As authorization needs got more complex, drove more identity data into the application domain
- Centralized Authorization Service external from applications that supports entitlement modeling & fine-grained authorization
  - Fine-grained entitlement modeling
  - Integration with Role Management
- Distributed, real-time, high performance Policy Enforcement Points
- Future support for incoming assertions

Authorization Service

Externalize, Centralize Authorization Policies



Agenda

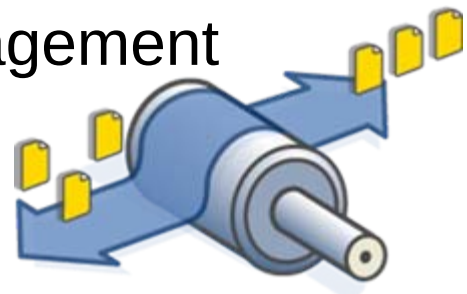


- Oracle Fusion
- Identity Management in Fusion Architecture
- Fusion Identity Services
  - Authentication Service
  - Identity Provider for SOA
  - Role Provider
  - Authorization Service
  - Provisioning

Provisioning

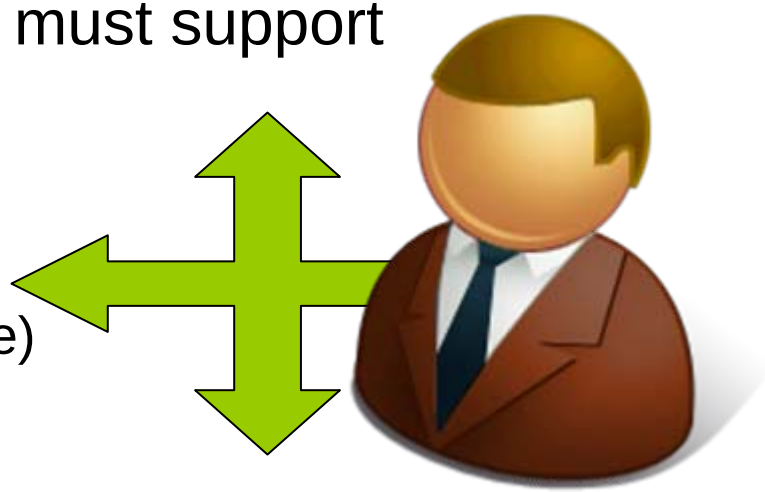
Centralize Identity Administration & Processes

- Service that supports administration of the IAM context
- Provides Identity and Account Provisioning
- Provides centralized policy administration and controls
  - Approval-based administration
  - Centralized policy enforcement (Auto-Provisioning, SoD)
  - Change notification mechanism
- Provides centralized self-service management
  - Profile Management
  - Password Management

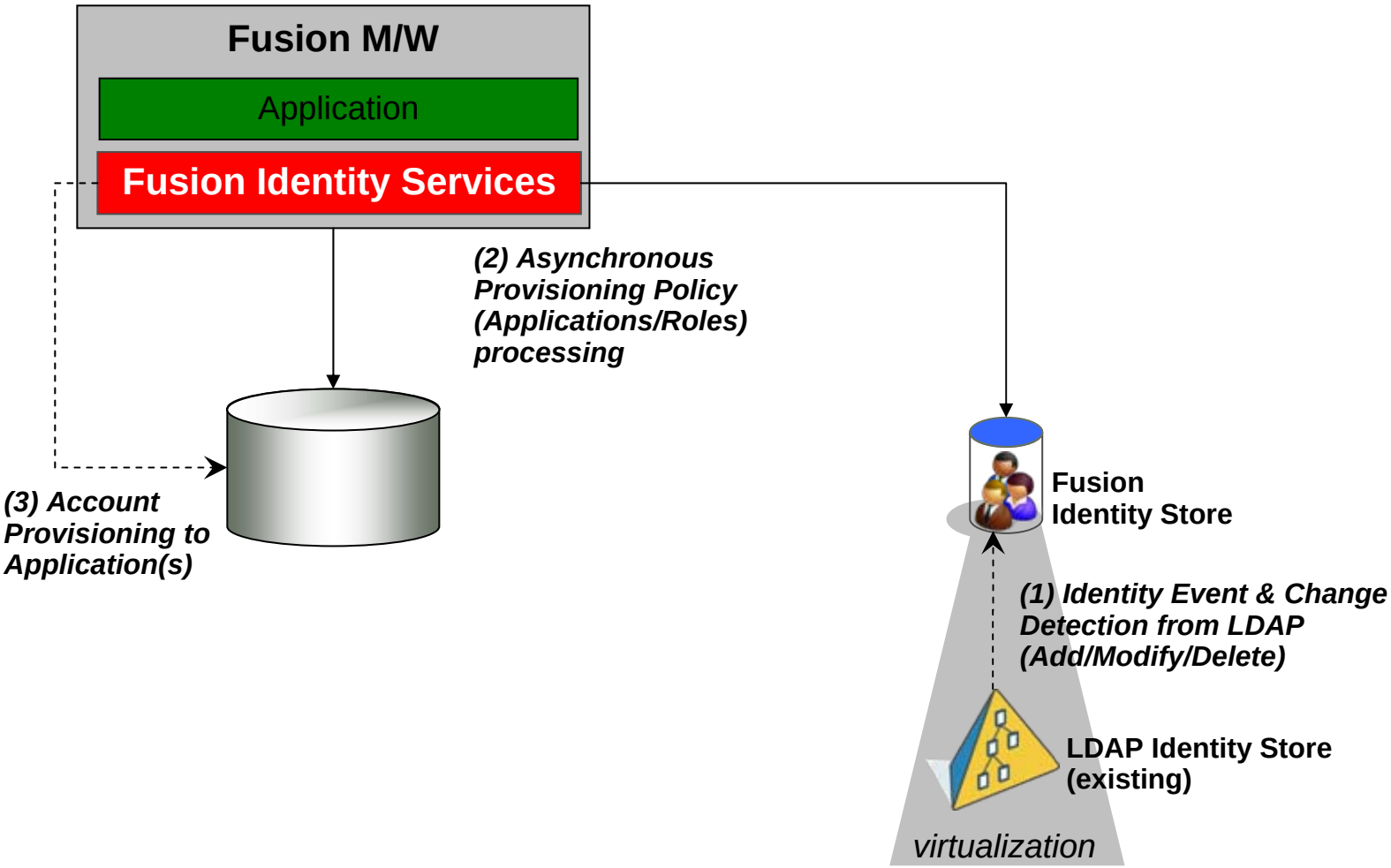


Identity Provisioning

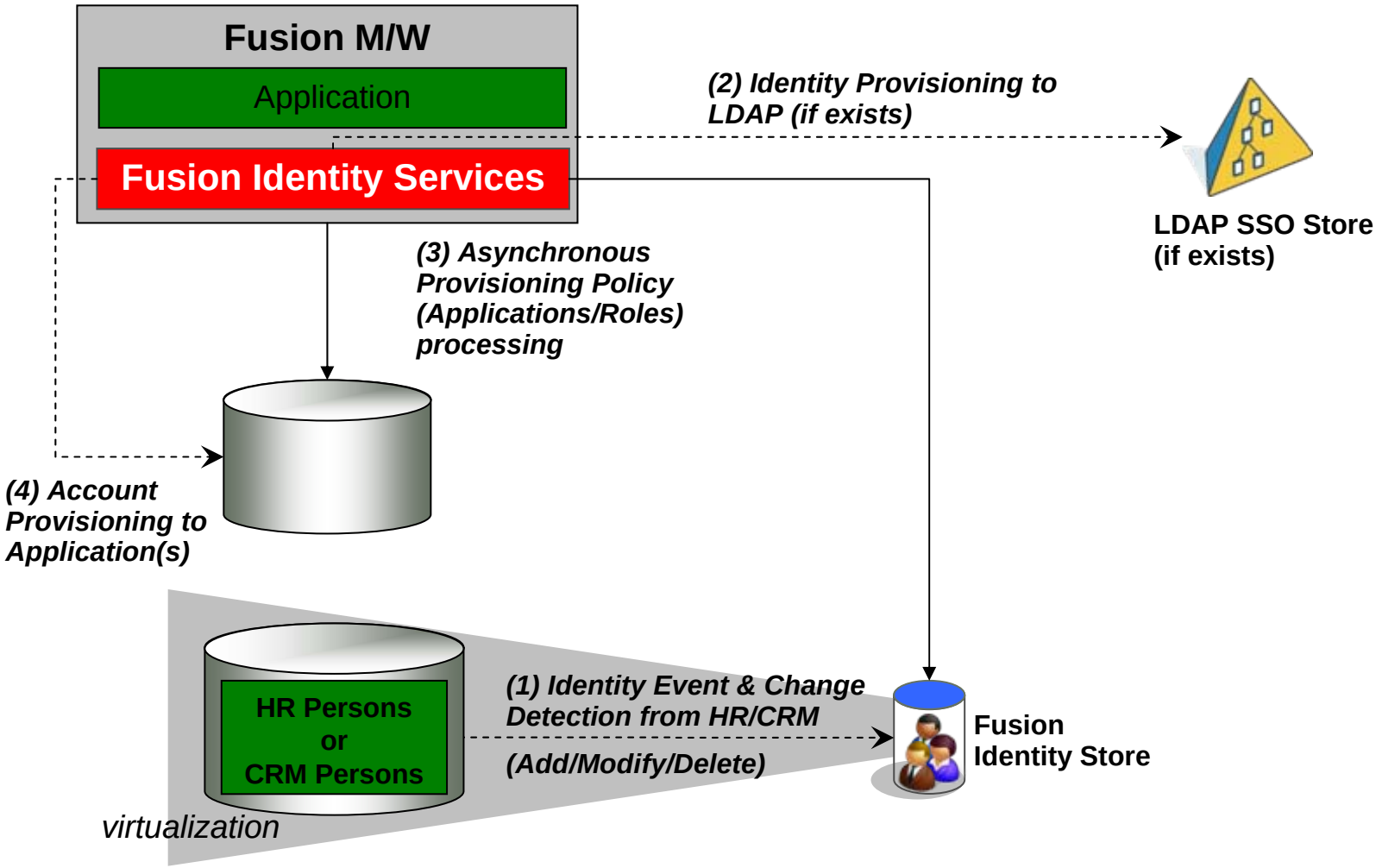
- Identity Provisioning Service ensures that identity information is properly set up in the environment, based on various authoritative sources
- The exact provisioning flows depend on the authoritative source of the identity in the deployment
- There are 5 sources that FIDM must support
  - LDAP
  - Fusion HR
  - Fusion CRM
  - Registration (Self or Administrative)
  - Enterprise IAM System



LDAP-Driven Identity Provisioning

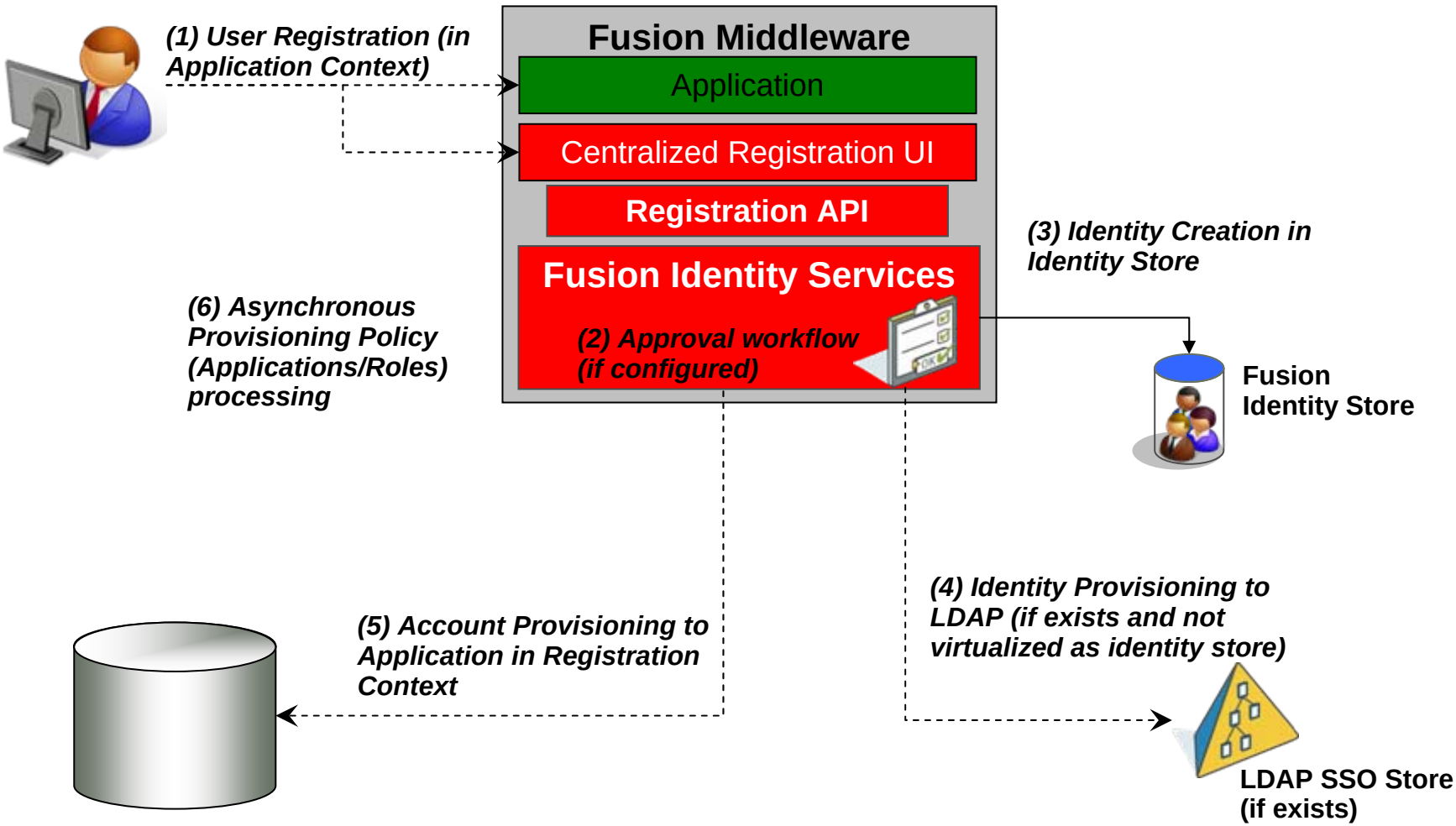


HR/CRM-Driven Identity Provisioning



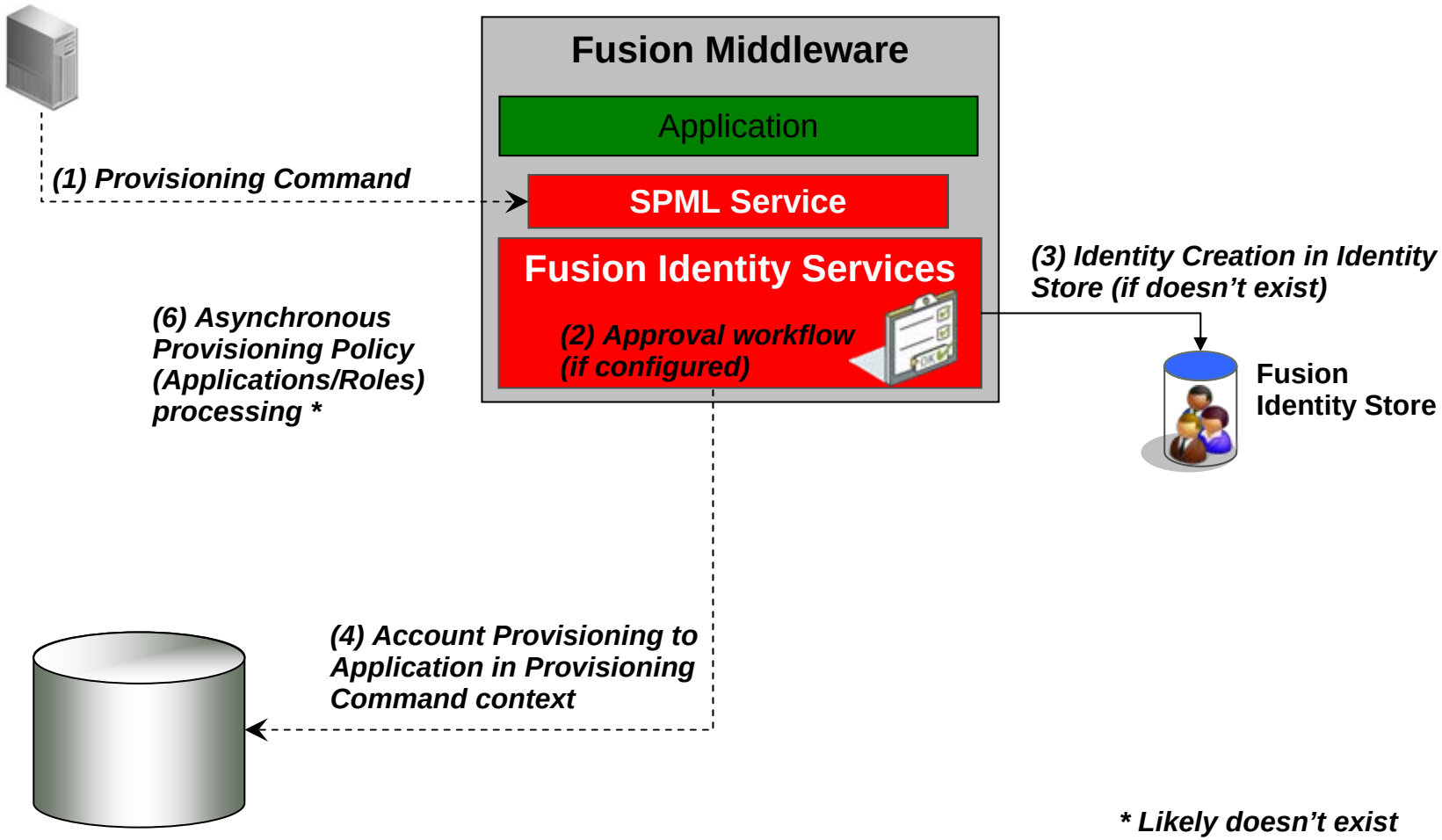
Identity Registration

Self or Delegated Administration

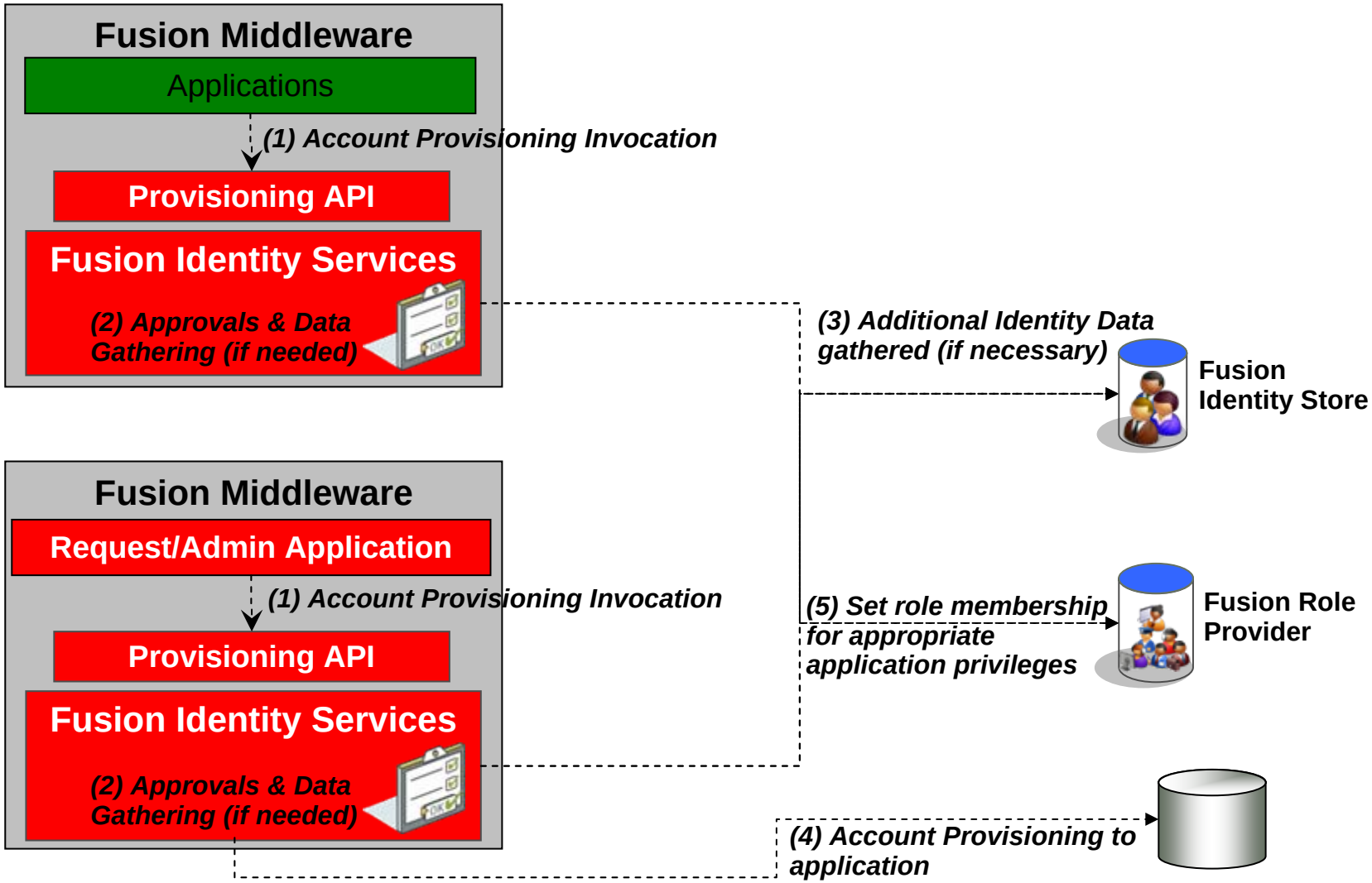


IAM-Driven Identity Provisioning

Excludes LDAP Identity Store Scenario



Account Provisioning



Self-Service Capabilities

Centralize Self-Service User Management

- Password Management
  - Single place to manage Single-Sign On password
  - Forgotten Password retrieval
    - Based on Challenge Response identification
  - Password Policies for strong passwords
    - Password History
- Profile Management
  - Maintain profile information
  - Primarily for Non HR/CRM led deployments
- Preferences Management

Self-Service Capabilities

Centralize Self-Service User Management

- Self-Service Request for Access
  - In new RBAC model, requesting access translates into a request for role membership
  - If user does not have an account (LUS entry) yet, implicit provisioning of account will take place
    - Supported by Just-In-Time gathering of profile data if not already available
    - Minimizes unnecessary data gathering

Policy-based Account Provisioning

- Rules based on Identity Attributes and Role Memberships
  - Determine accounts to provision
  - Determine roles to provision
- Automated
- Approval-based
- SoD compliant

In Conclusion

- Identity Services in Fusion Architecture will…
  - …reduce complexity through increased ability to leverage critical identity data while removing the management and replication challenges
  - …increase security by providing centralized policy management and a controls framework that can dynamically mitigate risks
  - …create a flexible, adaptable, integrated platform on which to build applications

Continue the Dialogue On My Blog

http://www.talkingidentity.com

For More Information

Join us tomorrow:

Tuesday, November 13, 2007

12:-15 p.m. – 01:15 p.m.

Innovations in Identity Management and Fraud Prevention

Amit Jasuja, Vice President, Oracle

Location: Yerba Buena Center Auditorium

For More Information

ADDITIONAL SESSIONS

Other sessions of interest

- S291877 – Enterprise role management and identity management in practice
  - Tue, Nov 13, 4:45pm, Moscone West Rm 3006 – L3
- S292034 – Brokering of Trust and Fine Grained Authorization
  - Thu, Nov 15, 10:00am, Moscone West Rm 3006 – L3
- S292075 – Using Identity Management Standards to solve Business Problems
  - Thu, Nov 15, 1:00pm, Moscone West Rm 3006 – L3

PRODUCTS IN ACTION

Visit our demos in Moscone South

- Oracle Access Manager and Oracle Identity Federation
- Oracle Identity Manager
- Identity Audit and Compliance
- Oracle Enterprise Single Sign-On
- Oracle Directory Services
- Oracle Role Manager
- Oracle Adaptive Access Manager
- Oracle Identity Management Suite Manageability

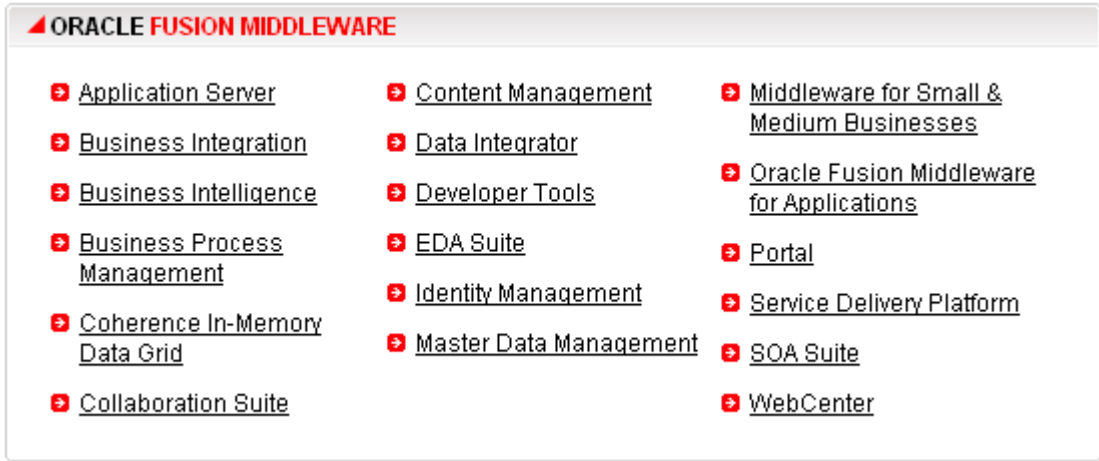
The No Slide Zone

- Innovations in Identity Management & Fraud Prevention
  - Tuesday, 12.15PM, Yerba Buena Center Auditorium

Learn More

www.oracle.com/middleware

- Whitepapers
- Webcasts
- Buyers Guides
- Analyst Reports
- Case Studies



- Podcasts

- Technical Information & Forums
  - **www.oracle.com/technology/products/middleware/index.html**

ORACLE IS THE INFORMATION COMPANY