



**ORACLE®**



## **Externalizing Identity**

Nishant Kaushik  
Principal Architect, Oracle Identity Management

# Also Known As

- Decentralized Identity
- The *other* Identity as a Service (IDaaS)
- Application-Centric Identity Management
- Identity Services
- The Evolved Identity Management Infrastructure

# The Premise

Lets think about the poor Application Developer

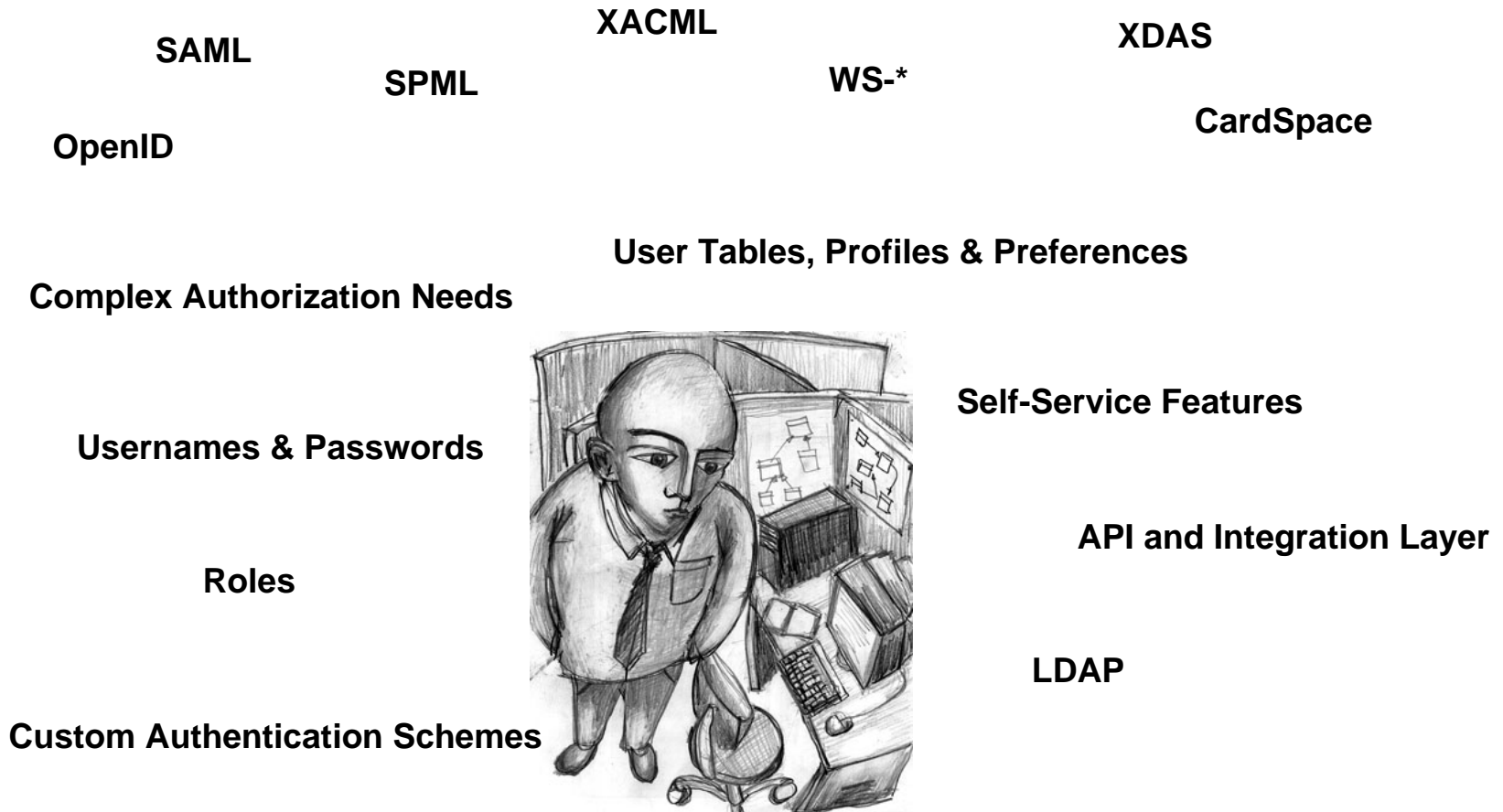


Image from <http://www.objectsandpixels.com>

# Oh, And Another Thing...

I would love to see exactly what is going on in there



# The Identity Equation

- Identity is an enterprise-wide concern that must...
  - ...be aligned with the strategic direction of the enterprise
  - ...be holistic in its coverage
  - ...help identify your “future state”
  - ...bring adaptability to your enterprise
  - ...satisfy technology, regulatory and business needs
  - ...introduce consistency and efficiency in IT infrastructure

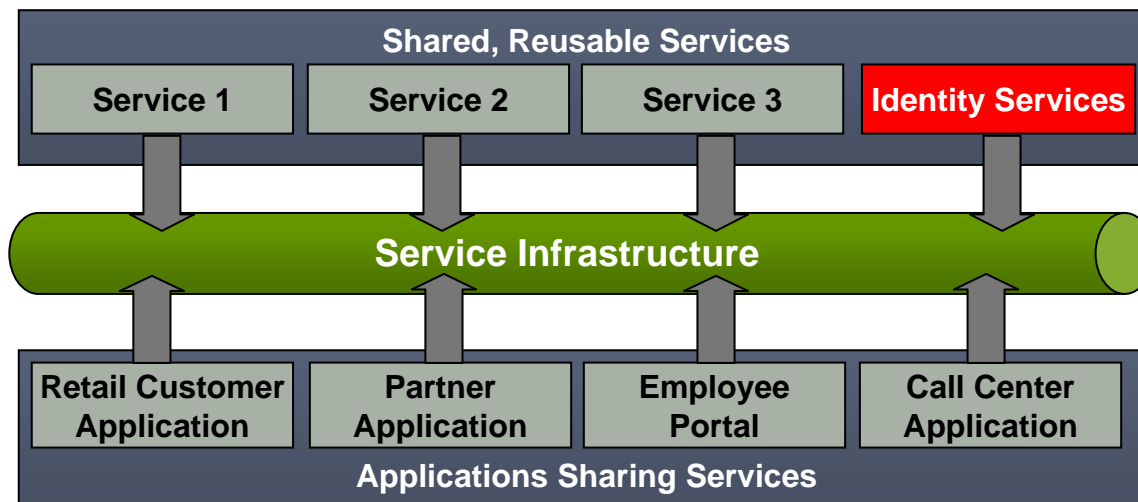
# Take 2 Aspirin and...

- We have to figure out a way to make identity mechanisms pervasive, simple and easy for developers to incorporate as part of application logic
- We need to define a framework of identity controls that gives businesses visibility and manageability of their security and compliance
- We must give power back to the owners of the identity data being used
- We must open up the infrastructure to adapt to incoming technologies



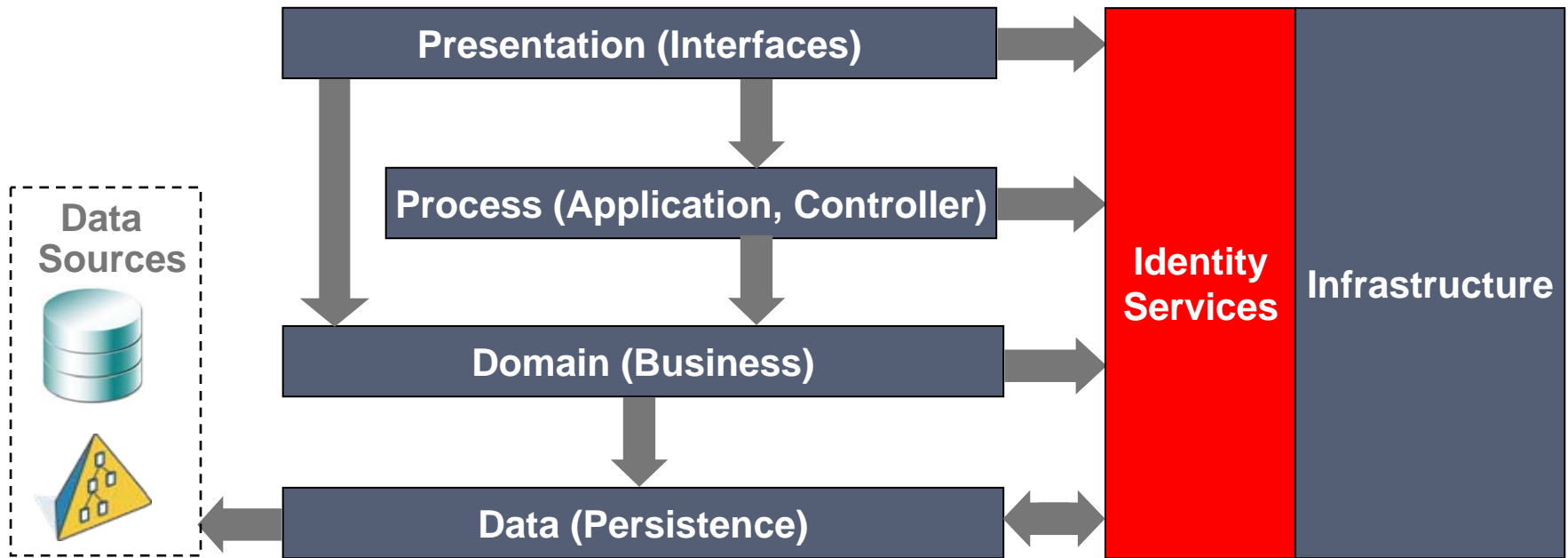
# Introducing Identity Services

- The goal: to devolve all those application identity silos into a common enterprise layer
- As organizations move towards SOA, identity components and management capabilities must be made available as a service in that architecture



# Enterprise Architecture with IDaaS

- Identity Services provide identity in a consistent, reusable way to all applications/services
  - Enables them to make identity an integral part of their business logic in a coordinated and meaningful way





# It's A Long Way Home

- IdM Vendors, Application Vendors and Customers must collaborate to define the Identity Services Layer
- Application Developers must adopt a SOA lifestyle
- Interoperability has to succeed
- Standards need to evolve
- We need to define an API model that makes development simple

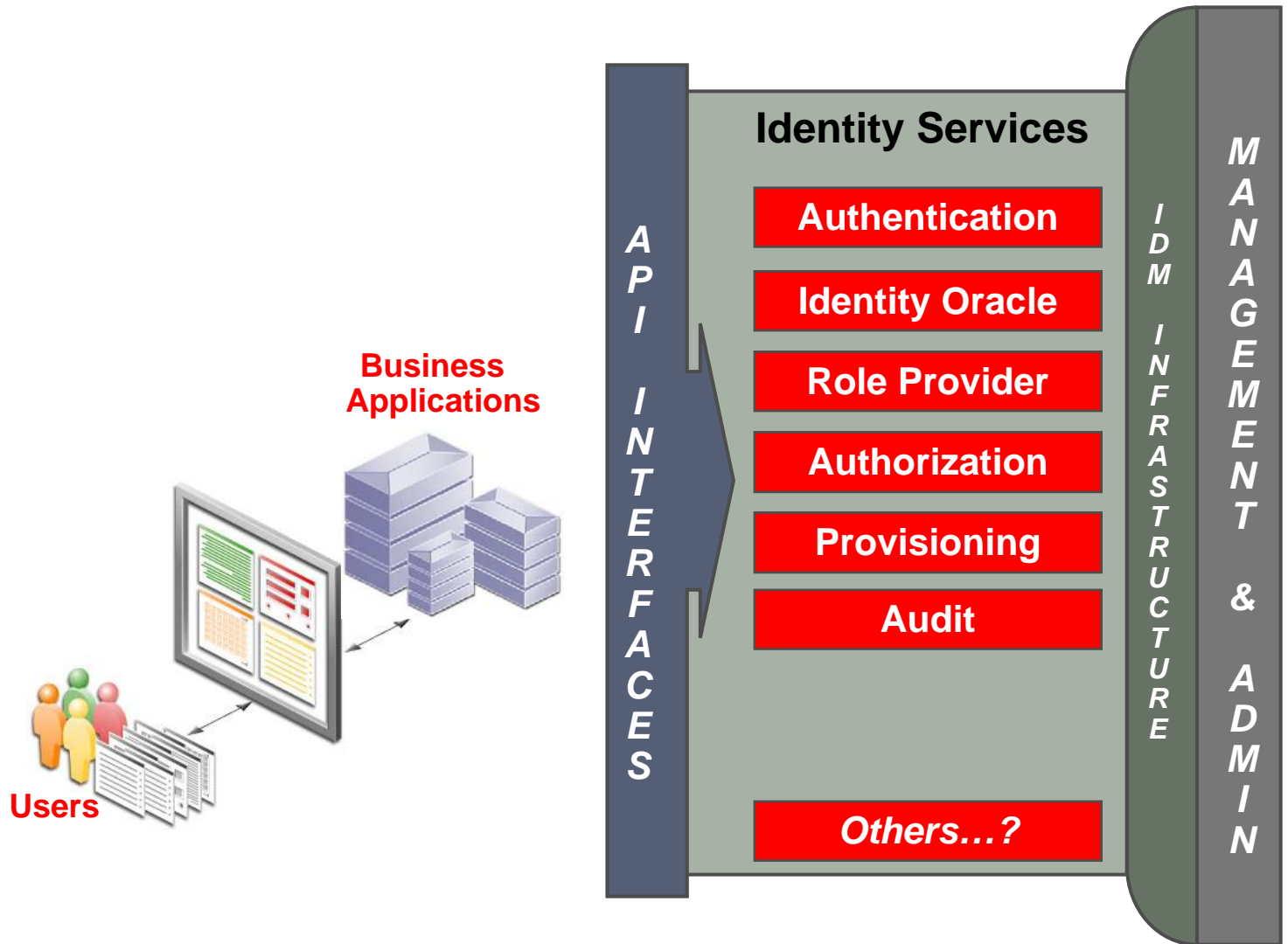


# First Things First

- We need to define what the identity services are and what capabilities they need to provide
- Keys to Success
  - Must satisfy concerns raised in the enterprise community as well as in the user-centric identity community
  - Balance de-centralization of identity with centralization of controls
  - Must leverage existing investment in IdM infrastructure
  - Must put the application development experience clearly in focus

***Build for Today, Architect for Tomorrow***

# The Identity Services Layer



# Authentication

## Externalize User Identification

- Service that provides the right level of assurance to the application of the identity of the interacting user
- State of the Art: SSO, E-SSO, Federation
- The API layer has evolved (JAAS) to remove a lot of the integration and tie-in problems (at least from the application developers plate)
- But...



# Authentication

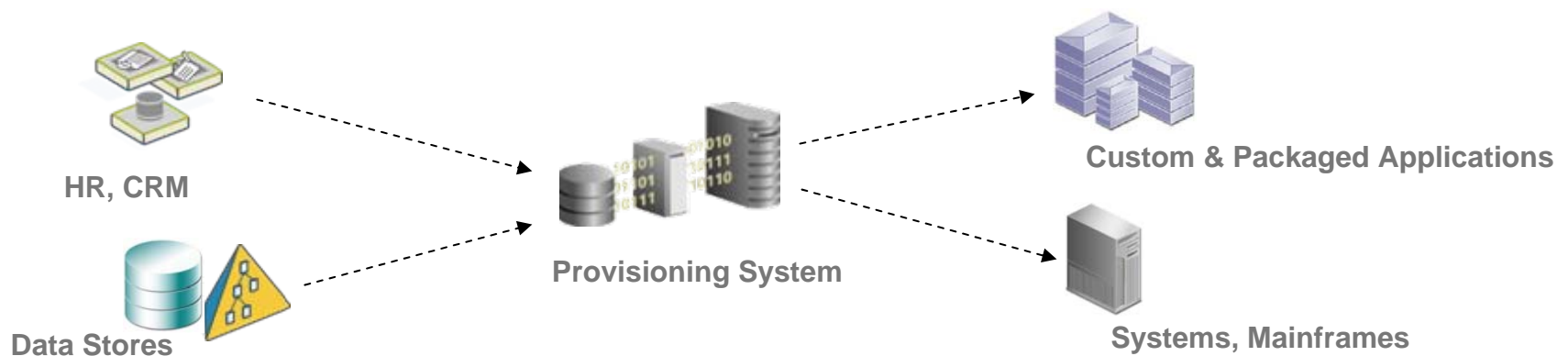
## Externalize User Identification

- The API layer is stuck with the simplistic binary idea of authenticated/unauthenticated
- OpenID, Cardspace emerging as Internet SSO tools
- Calls for Lightweight Federation based on user-centric technologies
- Multi-token authentication support w/ STS transforms
- Risk-based Authentication Levels
- Mutual Authentication

# Identity Oracle

## Externalize Identity Data

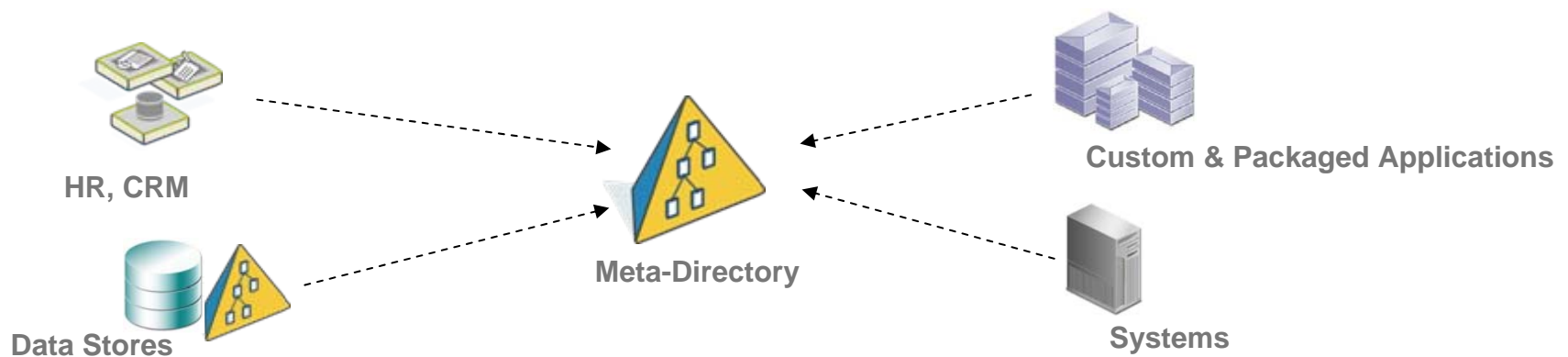
- Get away from those pesky User tables
- Multiple sources of Identity Data in the Enterprise
  - HR, CRM Systems, Custom Databases/Directories
- Replication into application user tables
  - Required deployment of costly provisioning tools



# Identity Oracle

## Externalize Identity Data

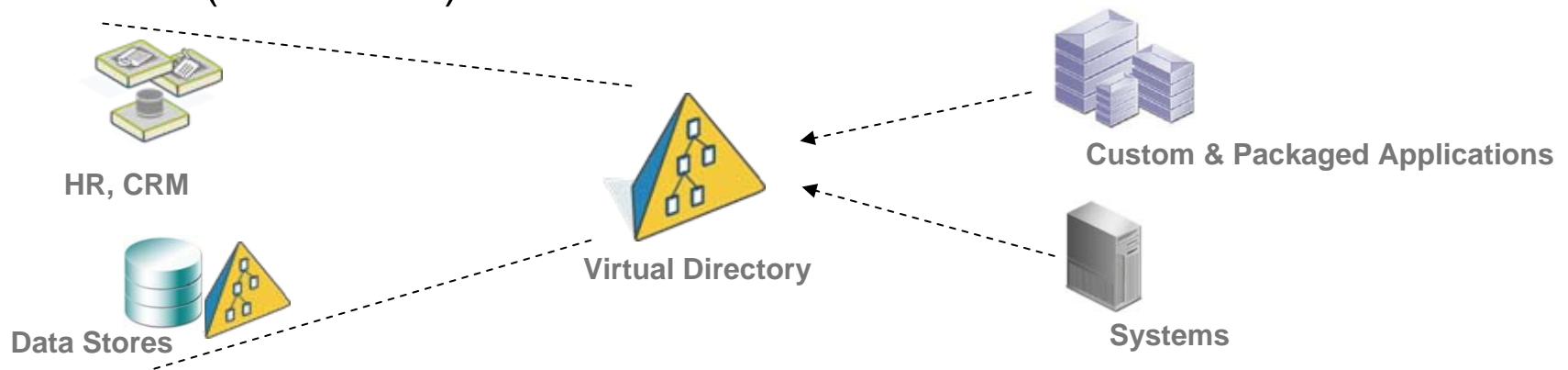
- Solution 1.0: Centralize Identity in Directory/Meta-Directory
- All applications must *speak* LDAP
- Identity data, by its nature, is de-centralized
  - Issues with maintenance, manageability, data freshness



# Identity Oracle

## Externalize Identity Data

- Solution 2.0: Virtualize Identity
- Leave identity data where it belongs
  - Provide a way to create complete profile by joining data
- Still
  - Applications must speak LDAP
  - Ignores some interesting identity sources: External IdP, The user (or DBKAC)

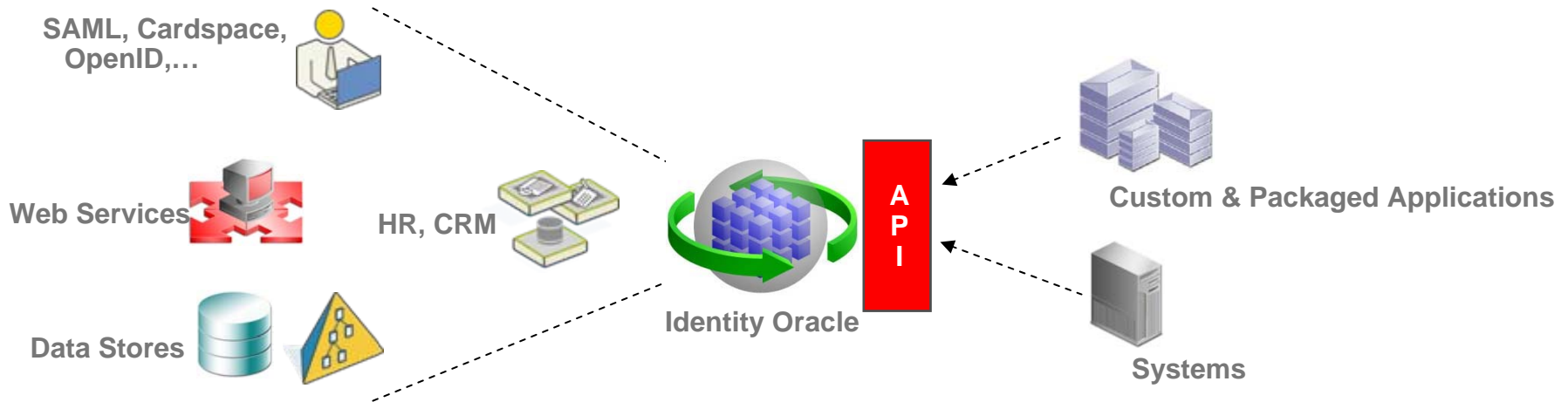




# Identity Oracle

## Externalize Identity Data

- Solution 3.0: Identity Oracle (Metasystem enabled)
  - Term coined by Bob Blakely of Burton Group
- Create complete identity profile across
  - Identity Applications, Identity Stores, Cloud Identity Providers, User-Centric Identity
- Provide developer friendly API



# Identity Oracle

## Externalize Identity Data

- Not an Identity Provider or Identity Attribute Service
- Implements the **principle of least knowledge**
  - Support both definitive (date of birth) and derived (over 21) identity data
  - Provide a Declarative Governance Model for how identity data is provided and consumed
    - Attribute declaration
    - Usage Constraints
    - Pub/Sub Models
    - Privacy, Regulations, Compliance
  - Schema Mapping
  - Translation layer

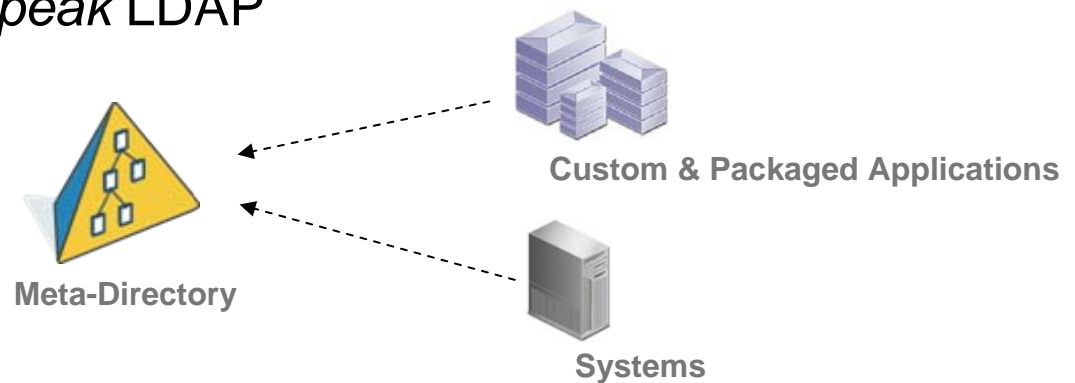


Check out Bob Blakely's podcast: [http://podcast.burtongroup.com/ip/2006/06/identity\\_and\\_co.html](http://podcast.burtongroup.com/ip/2006/06/identity_and_co.html)

# Role Provider

## Externalize Roles & Role Management

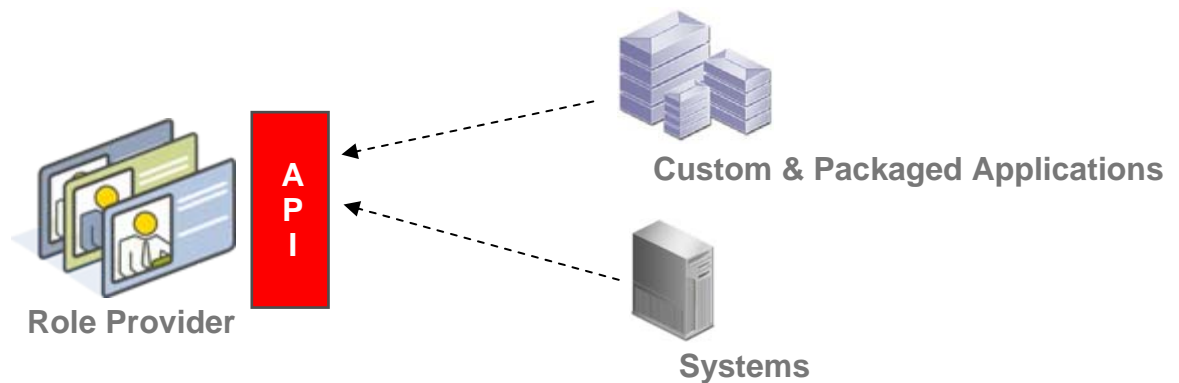
- Roles are necessary abstraction to make management manageable
- Service that provides information on roles and role memberships
- Enables heterogeneous RBAC adoption
- Version 1.0: LDAP Groups as Enterprise Roles
  - All applications must *speak* LDAP
  - Too simplistic



# Role Provider

## Externalize Roles & Role Management

- Version 2.0: Centralized Role System
  - Provide Enterprise Roles
  - Support Application Roles
  - Inheritance Hierarchies
  - Session Roles
  - Context-Sensitive Roles
  - Standards needed



# Authorization

## Externalize Authorization Policies

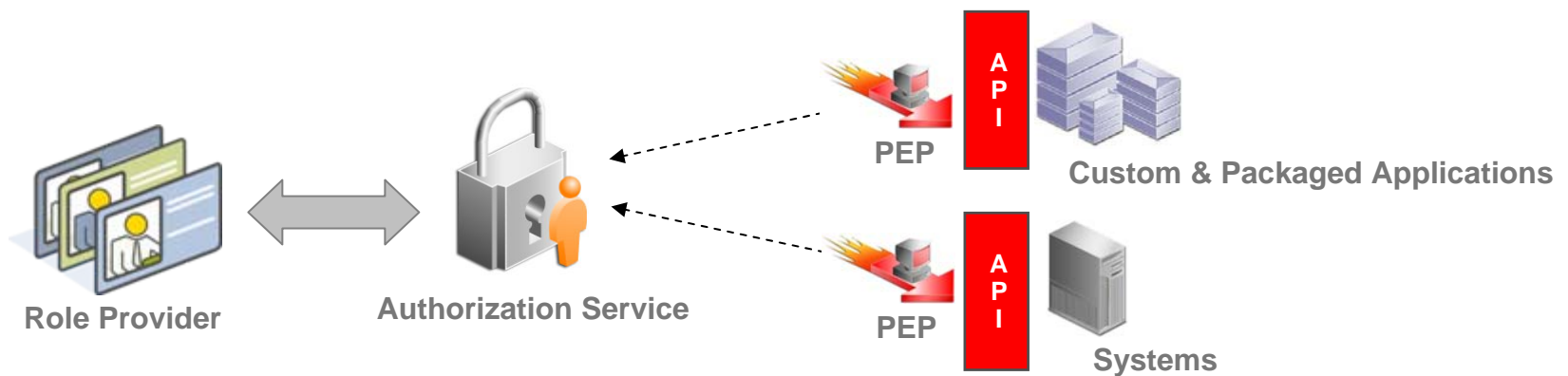
- As authorization needs got more complex, drove more identity data into the application domain
- External Authorization Service that supports entitlement modeling & fine-grained authorization
- Services focus from the beginning
  - Emerged from the XACML standard
- Aka Entitlement Management



# Authorization

## Externalize Authorization Policies

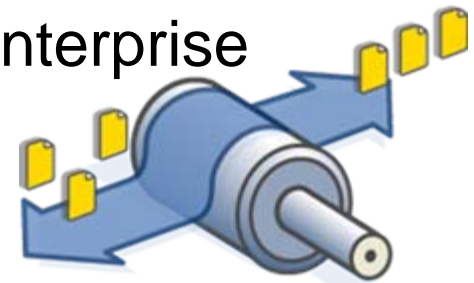
- Centralized control
  - Fine-grained entitlement modeling
  - Integration with Role Management System
- Distributed, real-time, high performance Policy Enforcement Points
- Support for incoming assertions



# Provisioning

## Externalize Identity Administration & Processes

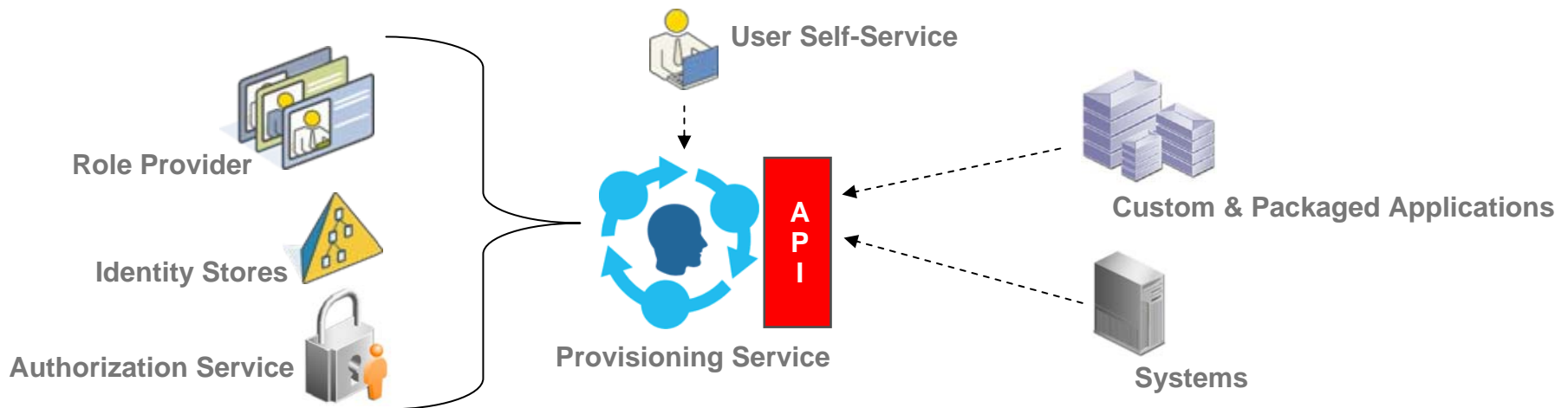
- Service that supports administration of the IAM context
- Turns the current model inside out
  - Current provisioning tools started as pure data flow
  - Added business controls (policies, workflow) by necessity
  - Going forward: Eliminate the data flow, not the controls
- Provisioning (as we know it) will change dramatically over time
- Needed to supports the fluid, ad-hoc enterprise



# Provisioning

## Externalize Identity Administration & Processes

- Provides centralized policy administration and controls
  - Approval-based administration
  - Centralized policy enforcement (Auto, SoD)
  - Change notification mechanism
  - End-user empowerment

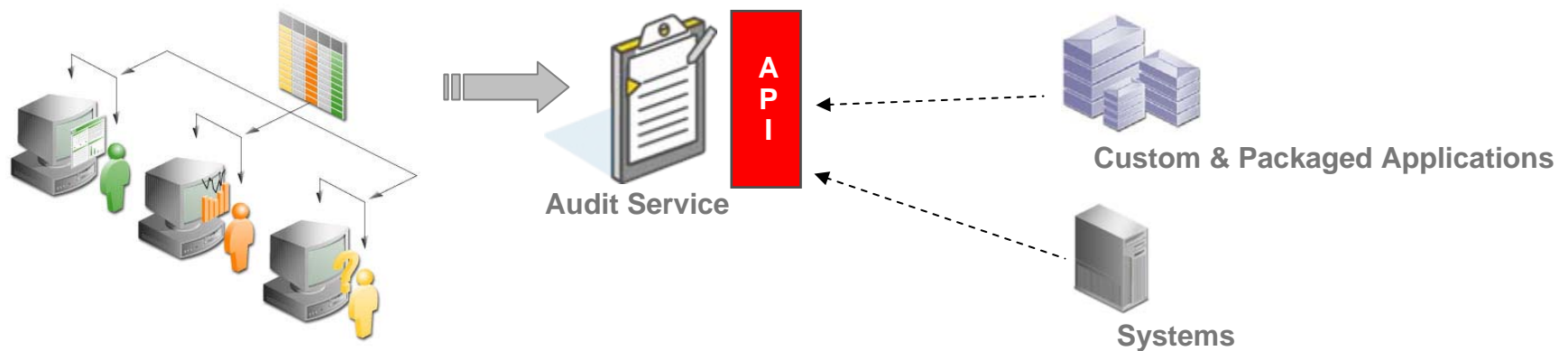




# Audit Service

## Externalize Identity Event Auditing

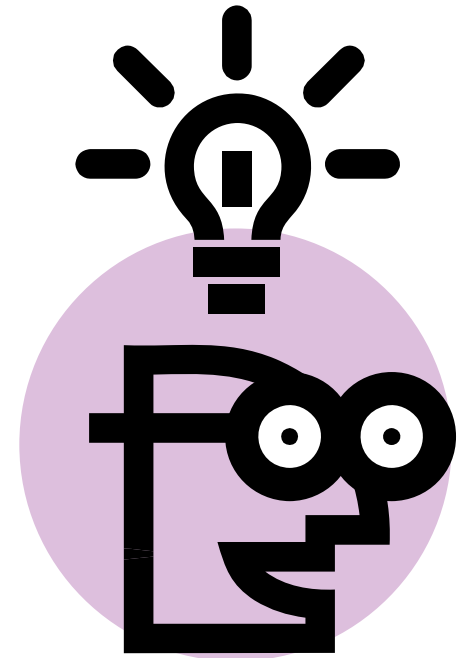
- Service that provides common audit service for all identity events
- Can hook into a centralized/distributed repository
- Provide de-normalization of audit data
- Enables: Event Correlation, Audit Trails, Activity Monitoring, Fraud Detection



# API Interface

## Developer Friendly Abstraction Layer

- Sits on top of standards based service providers
  - Vendor independence is key
- Provides a programmatic interface that is easy to use
- IDE integration
- Wait a minute...
- *Can the model be Claims-based?*



# Other Services...

- Claims Transformer
- Relationship Service
- ...?



# Caution!

- All of this is very new
  - Vendors take time to shift
- Getting developers to change their style is hard
  - SOA not as prevalent as was expected
- Disruptors
  - Mobile Computing
  - Disconnected Computing
  - Regulations



# Roadmap to IDaaS

- Still early stages, but a lot can be done today
- Enterprises
  - Measure your IdM maturity level (*see appendix*)
  - Embrace the SOA lifestyle
  - Identify identity sources and virtualize an enterprise identity profile
  - Document and put in place processes to govern management and use of identity information
  - Get involved! (*see appendix*)
- Vendors
  - Work on the standards needed for identity services
  - Adopt a services-focus in IAM products
  - Make the person part of the process

# Peace on Earth

- Identity Services 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
  - ...makes new types of de-perimeterized, identity-based business functionality viable





**Continue the Dialogue On My Blog**

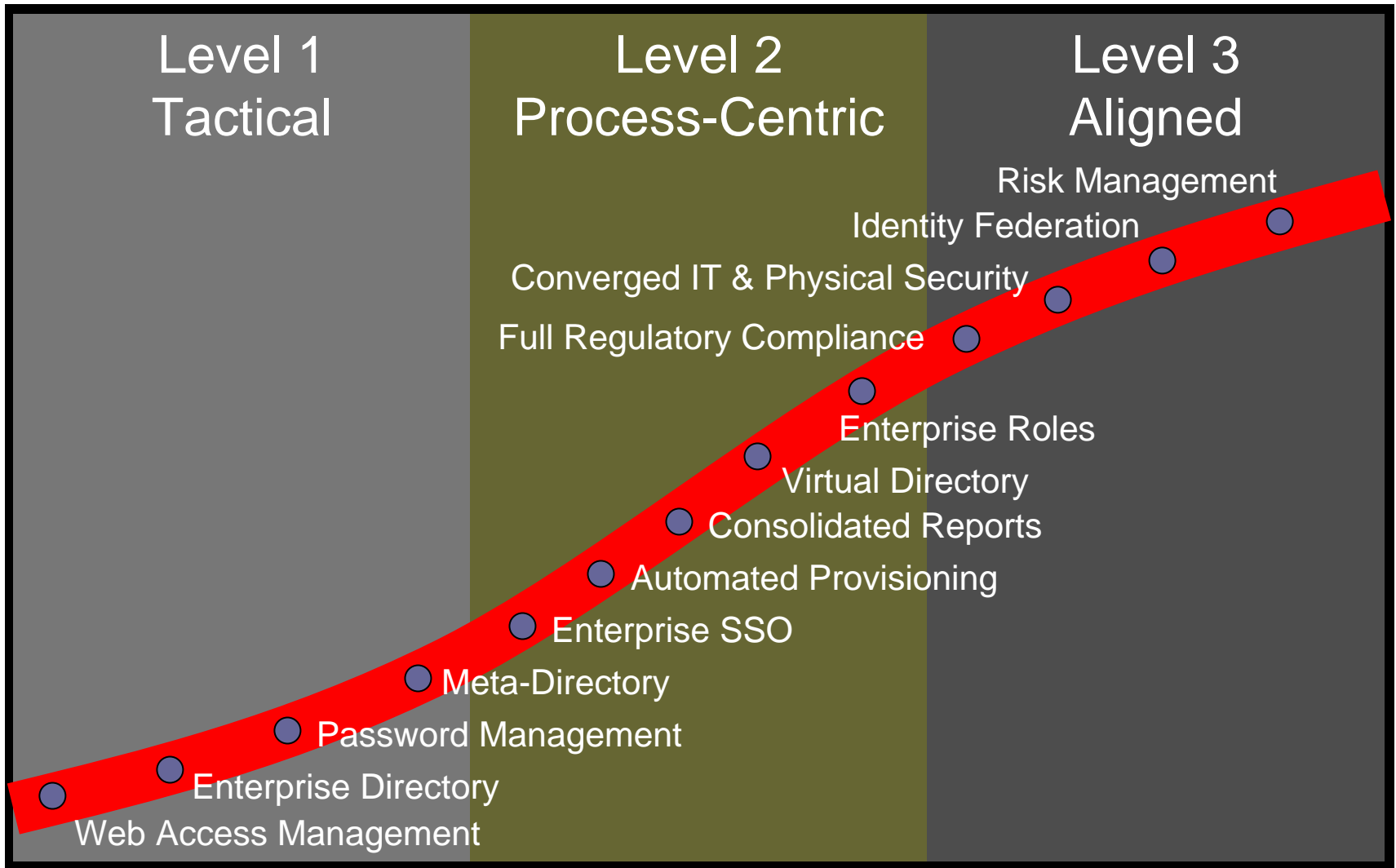
**<http://www.talkingidentity.com>**


# Appendix: Get Involved!

- Project Concordia
  - [http://projectconcordia.org/index.php/Main\\_Page](http://projectconcordia.org/index.php/Main_Page)
- Internet Identity Workshop
  - <http://iiw.windley.com/>
- Liberty Alliance
  - <http://www.projectliberty.org/>
- Burton Group's Identity Services Working Group
- Jericho Forum
  - <http://www.opengroup.org/jericho/>



# Appendix: Measure your IdM Maturity





The preceding 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.



**ORACLE IS THE INFORMATION COMPANY**