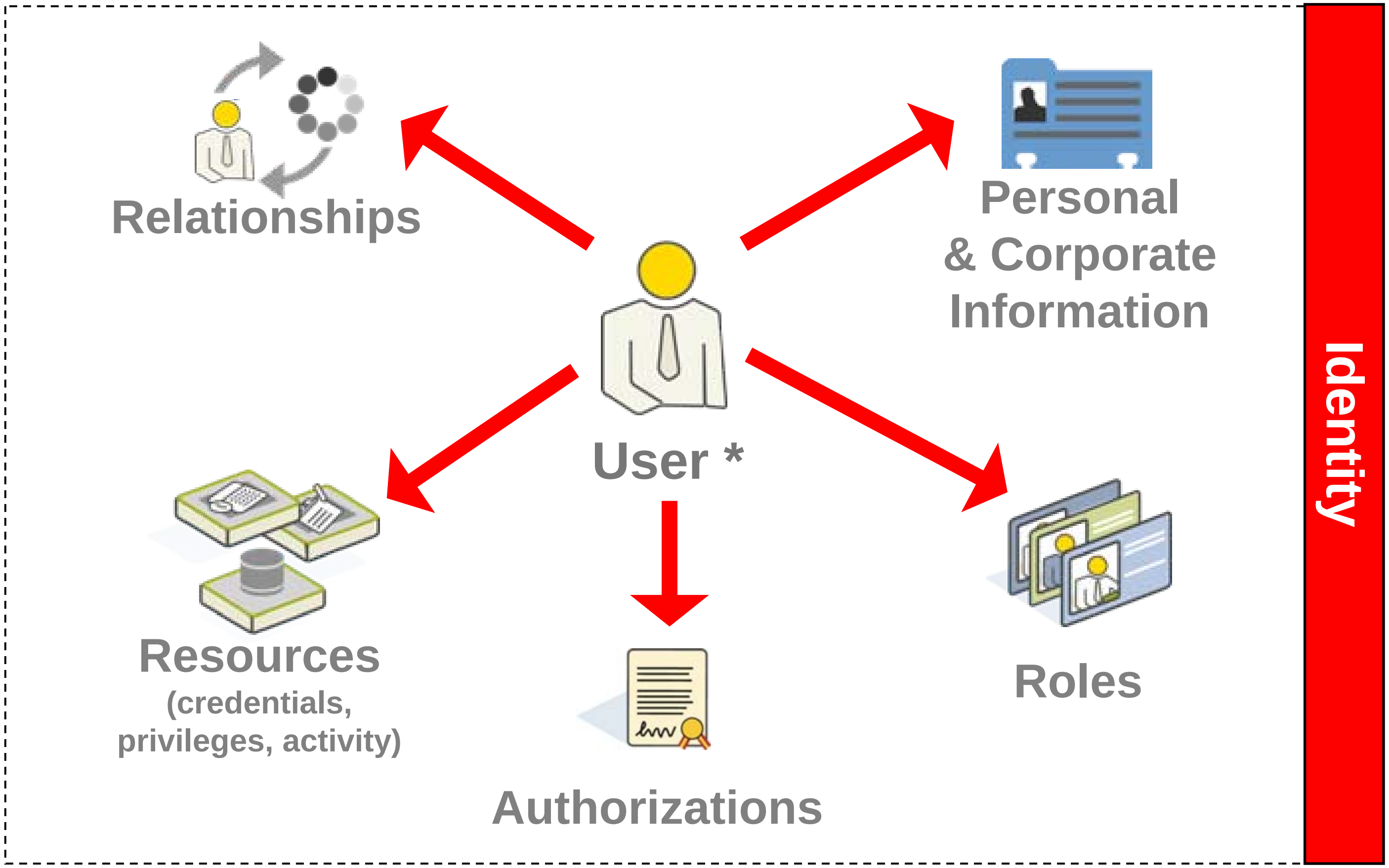
Understanding Identity as a Service

Nishant Kaushik
Principal Architect, Oracle Identity Management

Defining “Identity”



Relationships

Personal & Corporate Information

User *

Resources (credentials, privileges, activity)

Authorizations

Roles

Identity

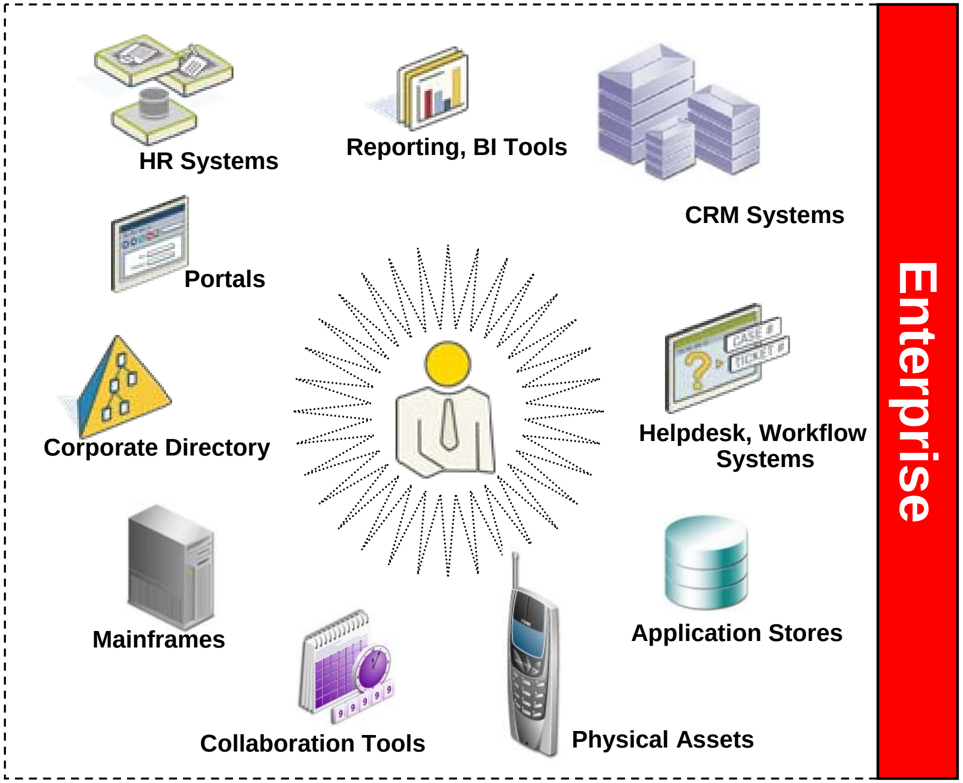
*** Let’s not forget non-human users (machines, services,…)***

Identity is Everywhere

Ubiquitous, Distributed, Fragmented, Duplicated

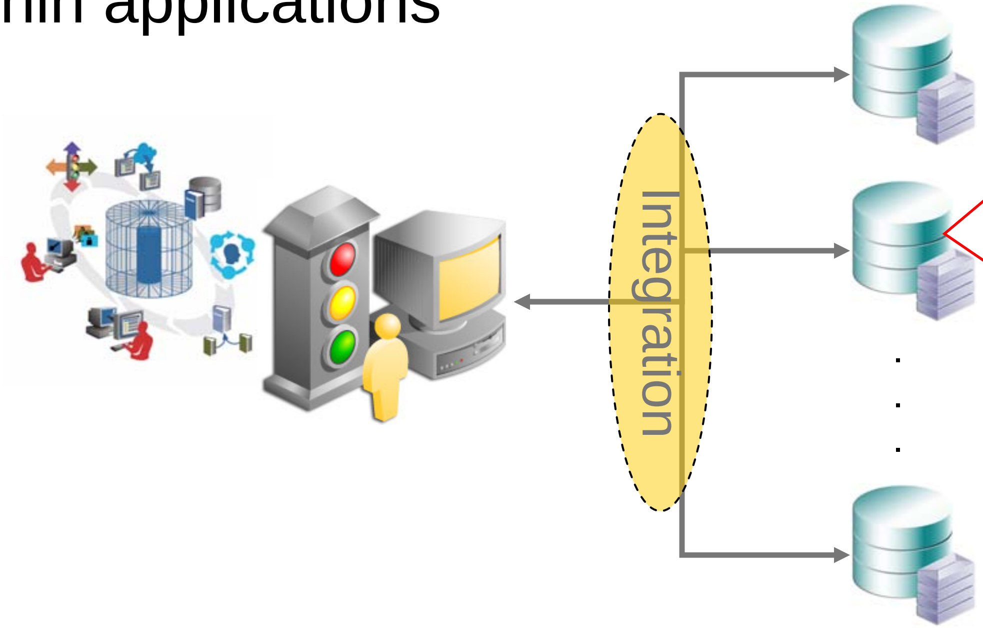
Every application/physical asset holds a bit of information about enterprise identities

- Identity is key to the operation and delivery of business services
- The data that comprises an identity comes from multiple sources, and is constantly in flux



Identity Management is Too Complex

- Today, Identity Management follows a classic “Systems Management” pattern, tying together through integration the various IAM silos that exist within applications

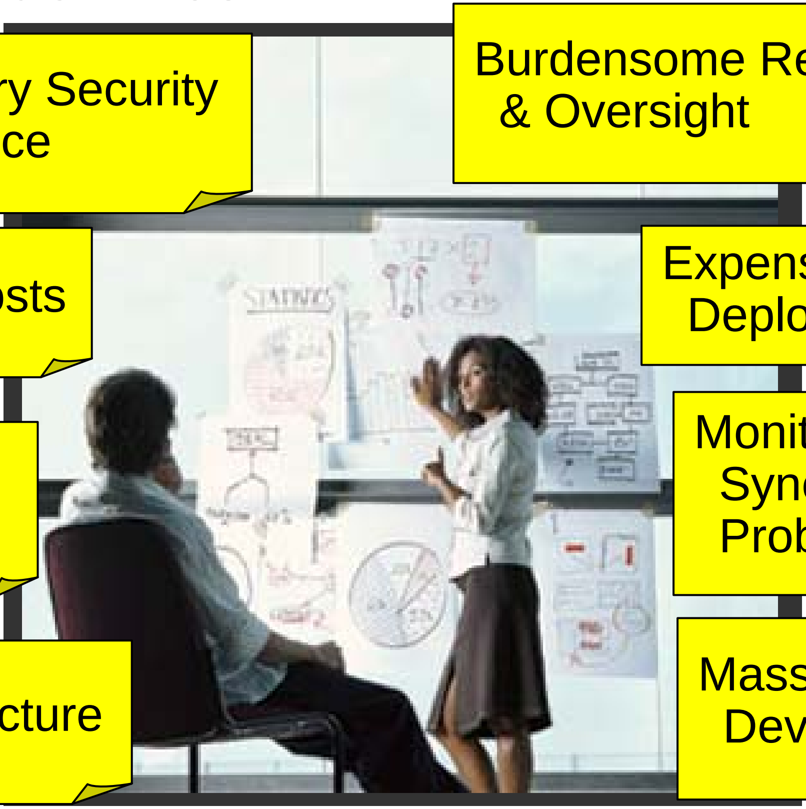


Application IAM Functionality

- **User Tables**
- **User ID & Password Stores**
- **User Profiles & Preferences**
- **Custom authentication schemes**
- **Complex authorization needs**
- **Profile & Password Management**

Identity is Causing Headaches ☺

- Enterprises must deal with complex challenges in managing Identities



Unsatisfactory Security & Compliance

Burdensome Regulations & Oversight

Integration Costs

Expensive IdM Deployments

Complex Audit Frameworks

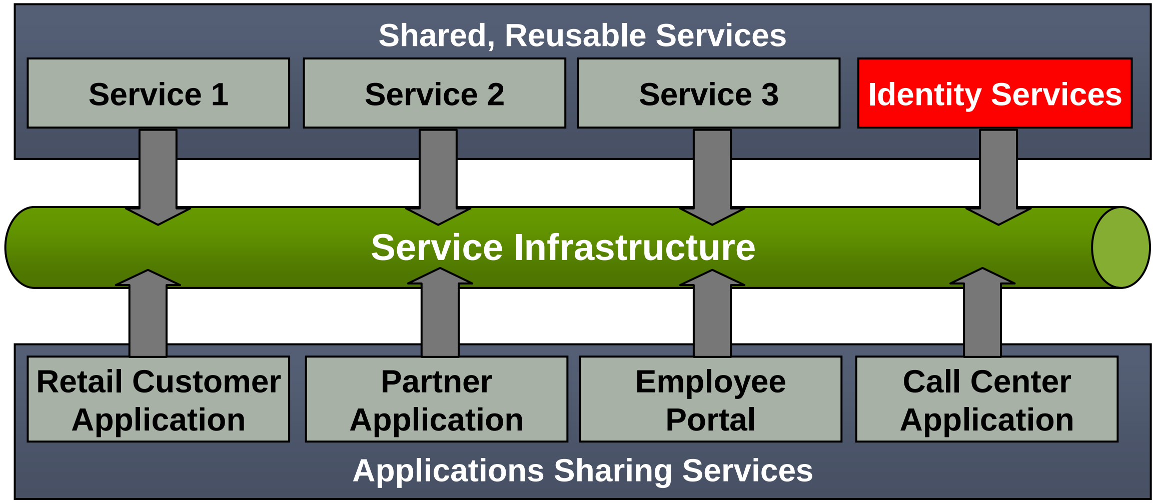
Monitoring & Synchronization Problems

Costly Infrastructure

Massive Design & Development Efforts

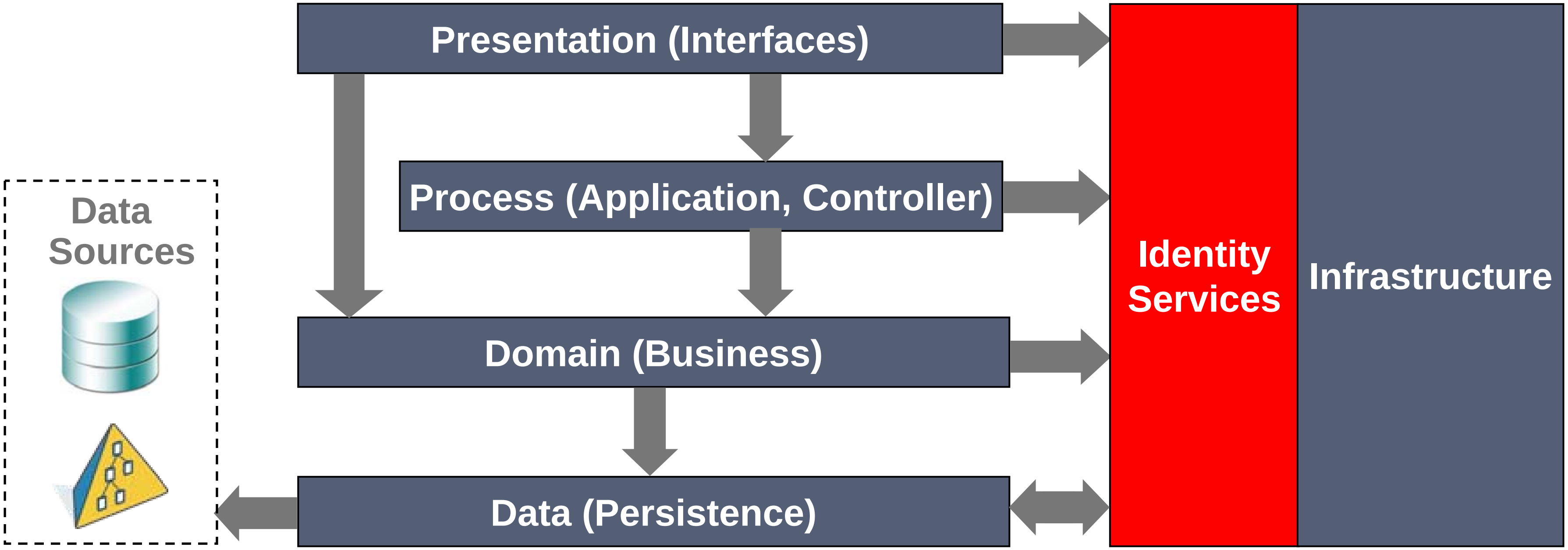
Introducing Identity as a Service

- 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

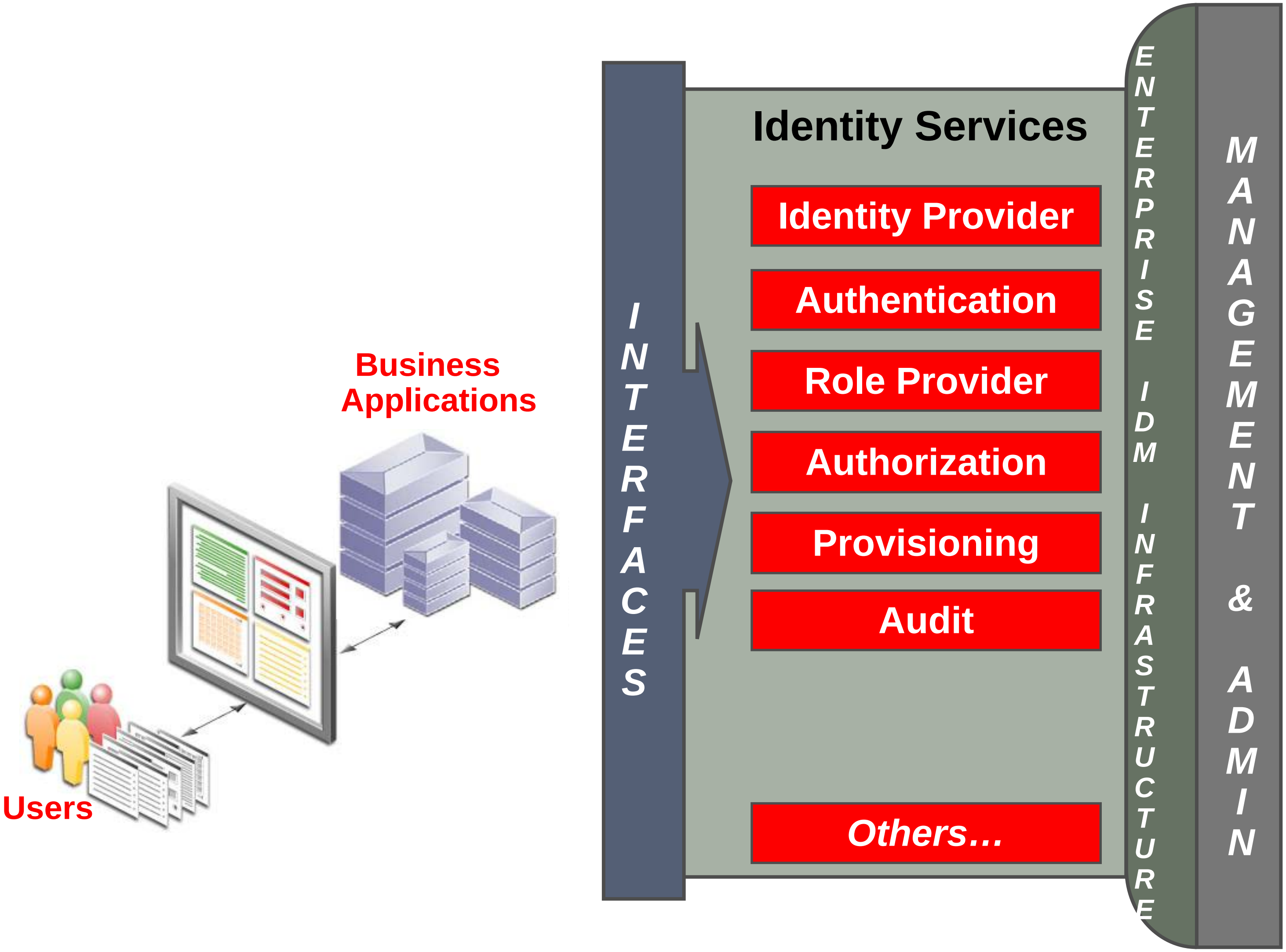
- Identity Services provide identity in a consistent, reusable way to all applications/services
  - Enables them to make identity an integral part of their business logic in a coordinated and meaningful way



Why Identity as a Service?

- IDaaS enables integration of identity services into application development and application runtime environments
  - Applications can now embed IAM functionality as part of their inherent business processes without having to code it themselves
- Conforms to the SOA approach to enterprise development, promoting loose coupling to ensure long term viability and heterogeneity of business solutions

The Identity Services Layer



Business Applications

Users

INTERFACES

Identity Services

Identity Provider

Authentication

Role Provider

Authorization

Provisioning

Audit

Others…

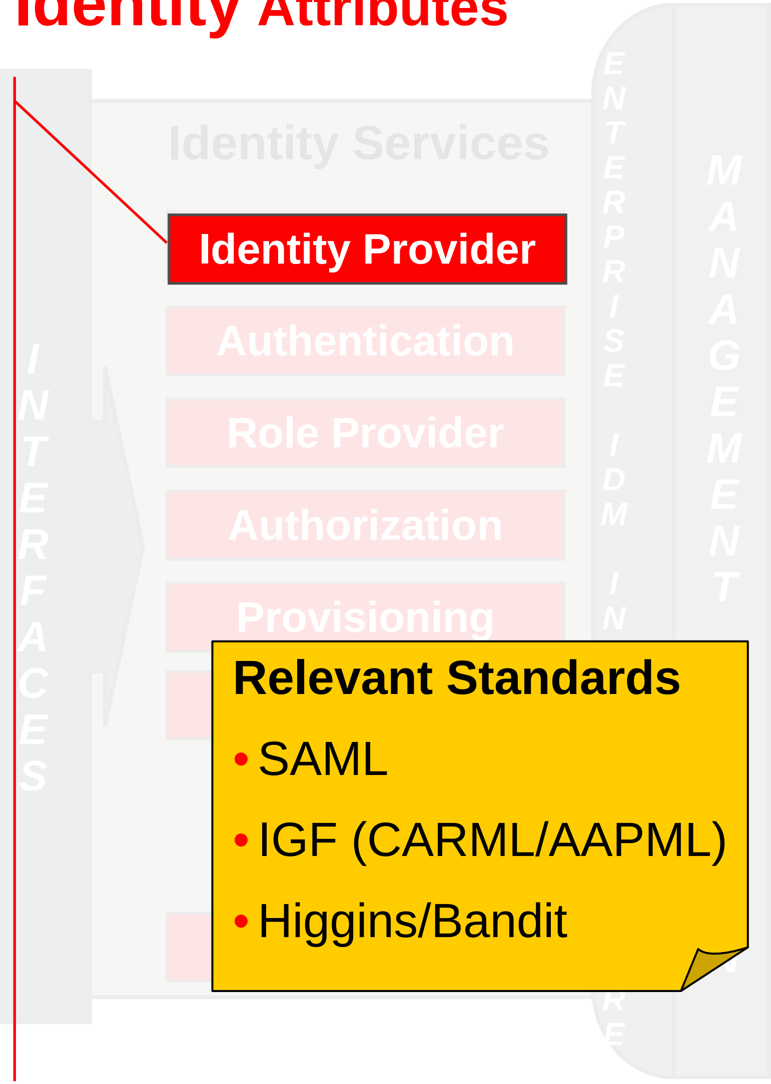
ENTERPRISE IDM INFRASTRUCTURE

MANAGEMENT & ADMIN

Identity Services in IDaaS

Identity Provider: Externalize Identity Attributes

- Service that provides access to identity profile data
- Approach has evolved over time
  - v1.0: Consolidation in Directory
  - v2.0: Virtualized view over multiple identity data sources
  - v3.0: Collaborative metasystem?
- Interesting Requirements:
  - GUID support
  - Support definitive (date of birth) and derived (over 21) identity data
  - Declarative models for both consumer and provider
  - Mapping/translation layer
  - Federation



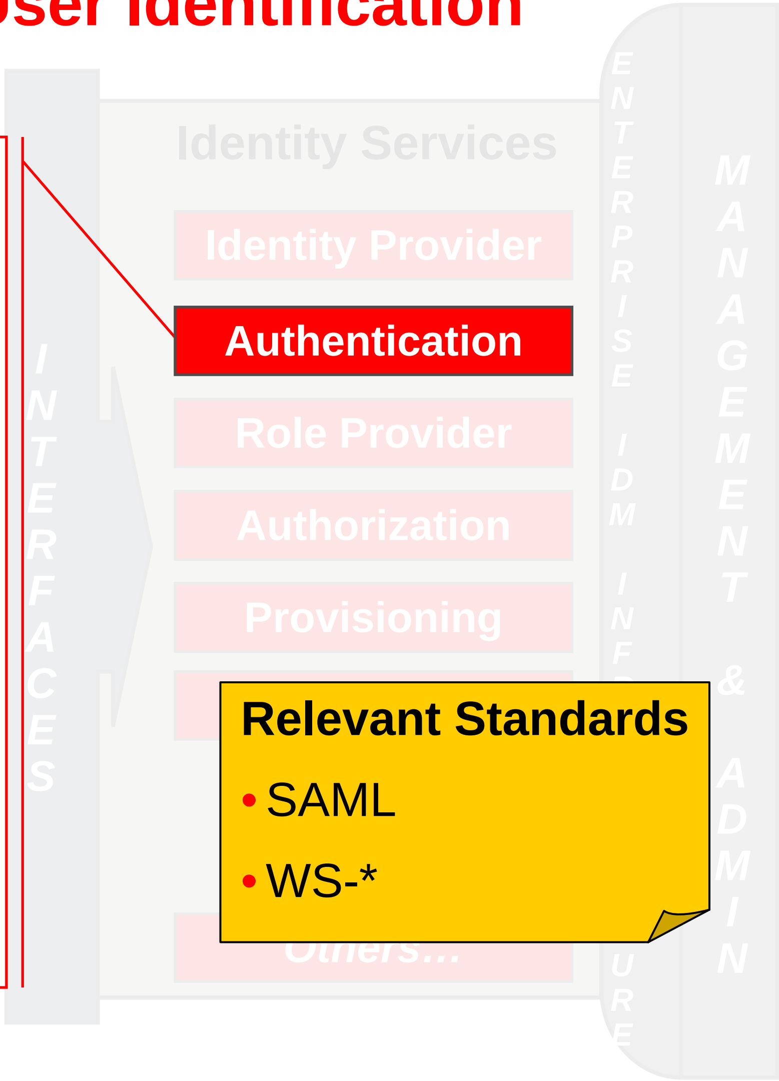
Relevant Standards

- SAML
- IGF (CARML/AAPML)
- Higgins/Bandit

Identity Services in IDaaS

Authentication: Externalize User Identification

- Service that provides identity authentication capabilities
- Current state of the art: SSO, eSSO, Federation
- Emerging user-centric identity technologies: OpenID, Cardspace
- Interesting Requirements
  - Multi-token authentication support
  - Security Token exchange Service (STS)
  - Graded Authentication Levels
  - Lightweight Federation



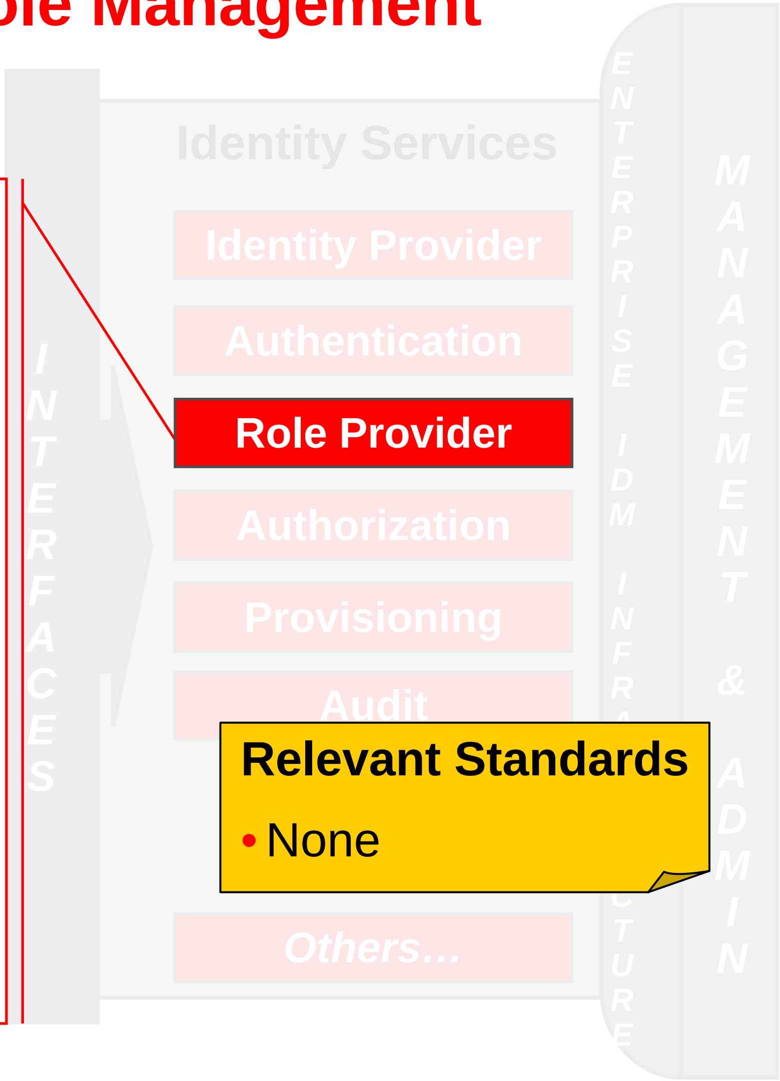
Relevant Standards

- SAML
- WS-*

Identity Services in IDaaS

Role Provider: Externalize Role Management

- Service that provides roles and role memberships
- Enables heterogeneous RBAC adoption
- v1.0: Treat Groups in Identity Directory as Enterprise Roles
  - Too simple for modern enterprise
- Interesting Requirements:
  - Support Enterprise Roles as well as Application Roles
  - Support context sensitive roles
  - Support session roles



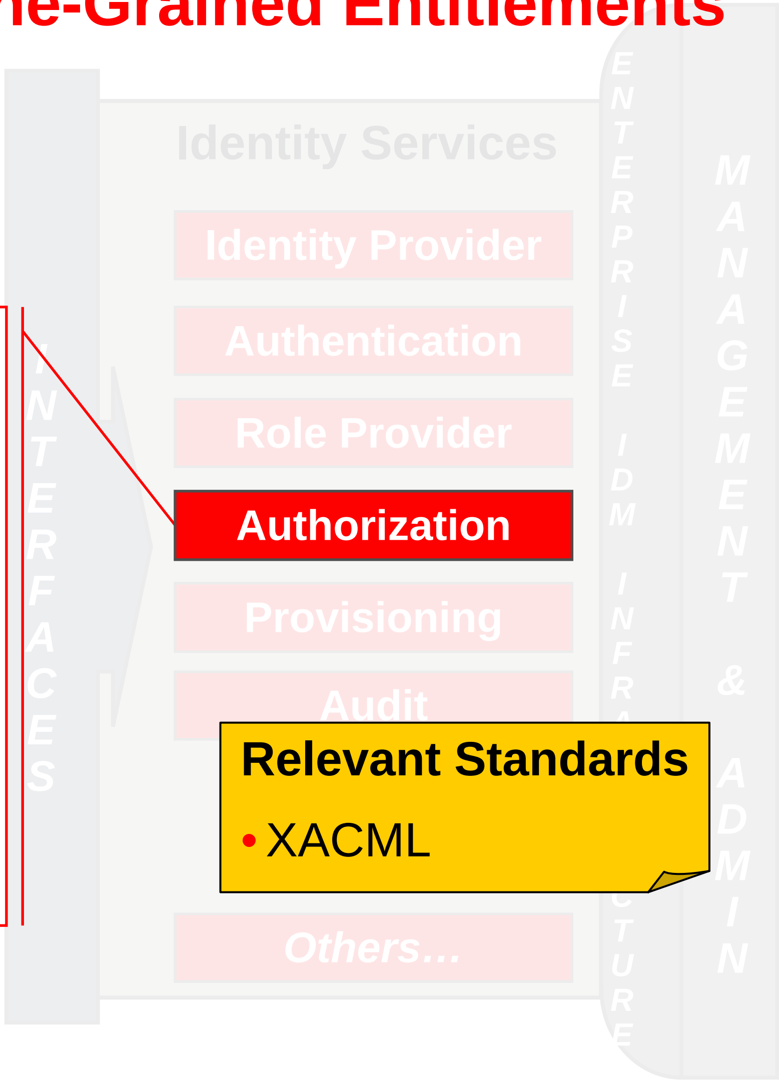
Relevant Standards

- None

Identity Services in IDaaS

Authorization: Externalize Fine-Grained Entitlements

- Service that supports entitlement modeling & fine-grained authorization
- Early stages
  - Started with the emergence of XACML standard
- Interesting Requirements:
  - Fine-grained entitlement modeling
  - Real-time, high performance Policy Enforcement Points



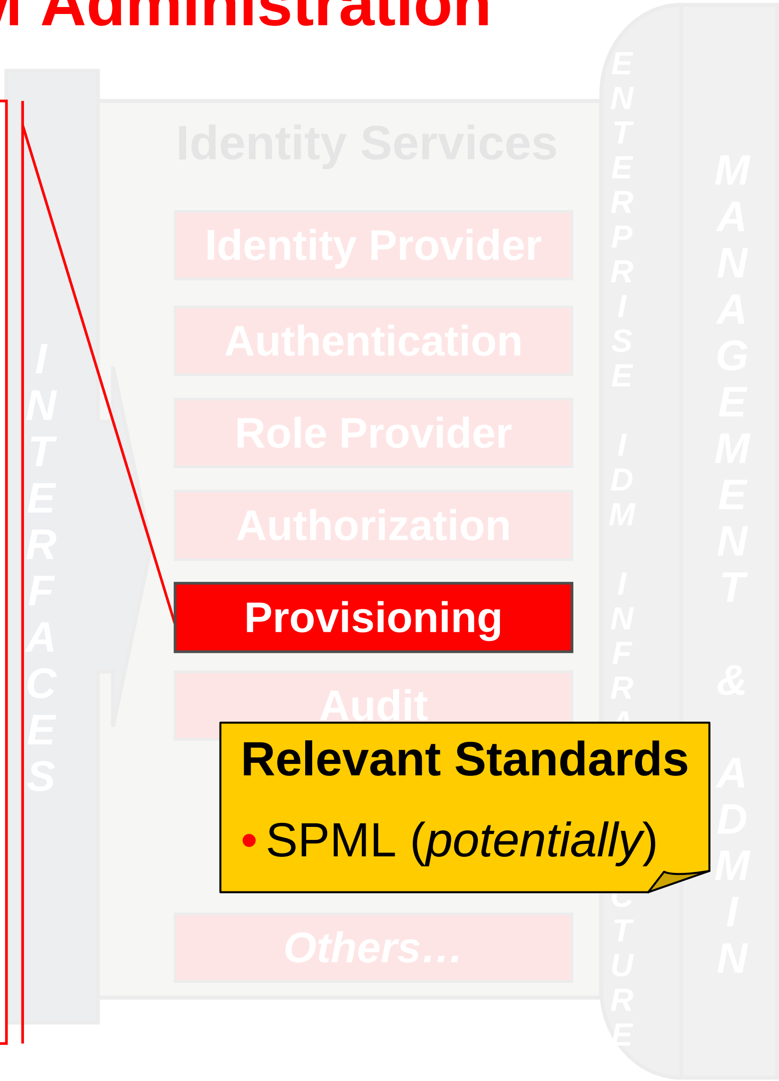
Relevant Standards

- XACML

Identity Services in IDaaS

Provisioning: Externalize IAM Administration

- Service that supports administration of IAM context
- Turns current model inside-out
- Provides centralized policy administration and controls
- Interesting Requirements:
  - Approval-based administration
  - Federated provisioning
  - Support local context
  - Centralized policy enforcement
  - Change notification mechanism
  - End-user empowerment
- Will change dramatically over time



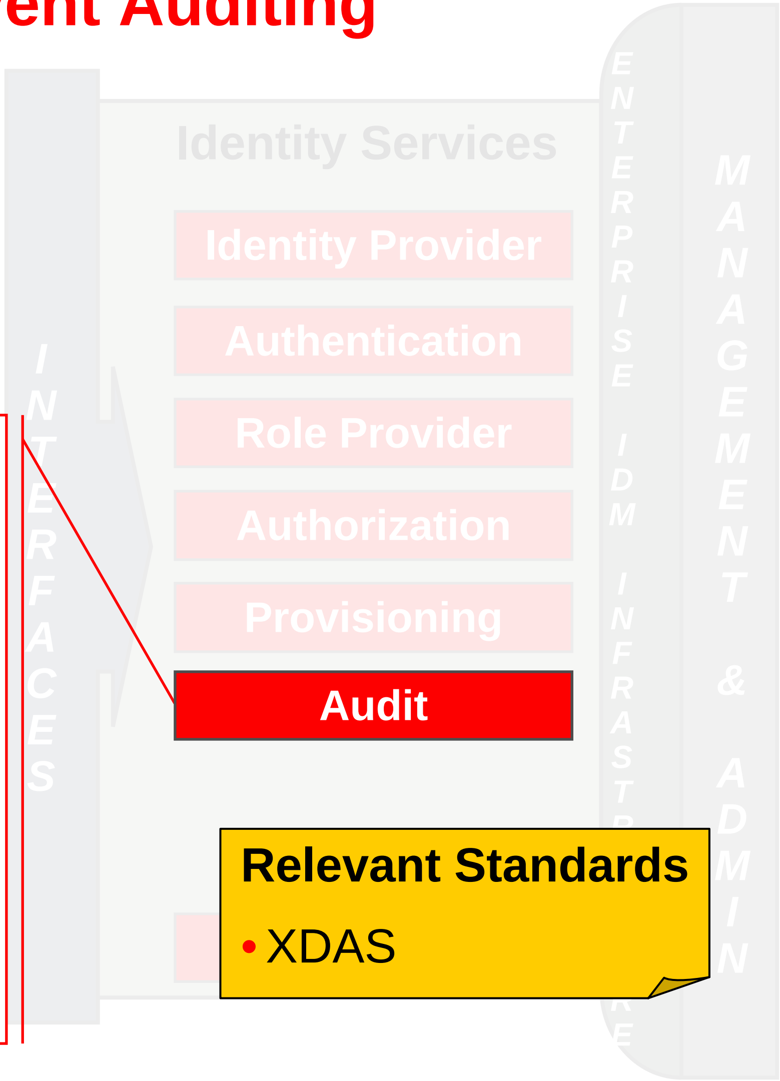
Relevant Standards

- SPML (*potentially*)

Identity Services in IDaaS

Audit: Externalize Identity Event Auditing

- Service that audits all identity events
- Provides centralized repository, de-normalization of audit data
- Interesting Requirements:
  - Event Correlation
  - Audit Trails
  - Activity Monitoring
  - Fraud Detection



Relevant Standards

- XDAS

De-Perimeterisation and IDaaS

DE-PERIMETERISATION

- Move security control closer to the source – to the end-points
- Be in total control of all users' access rights
- Be in control of the connecting device
- Add policies that dictate how and under what circumstances each user can access each service
- Make access "seamless" and base it on cooperation between applications and users and the use of secure protocols

▶

IDENTITY AS A SERVICE

- Maintain identity attributes at the source – avoid replicating it out unnecessarily
- Centralize role and identity policy management
- Establish standard-based policies for how applications connect to and use identity authorities
- Support a declarative system for identity usage that is based on application usage and environmental factors
- Make identity services part of your enterprise SOA platform, and use standards-based protocols where available

"What is De-perimeterisation" taken from the presentation "Secure Applications" by Tomas Olovsson at Jericho Forum Spring Conference 2007

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

Conclusions

- Identity must…
  - …be aligned with the strategic direction of the enterprise
  - …be holistic in its coverage
  - …help identify “future state”
  - …bring adaptability in the face of change
  - …introduce consistency and efficiency in IT infrastructure
- IDaaS will…
  - …reduce complexity through increased ability to leverage critical identity data while removing the management/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-perimeterised, identity-based business functionality viable

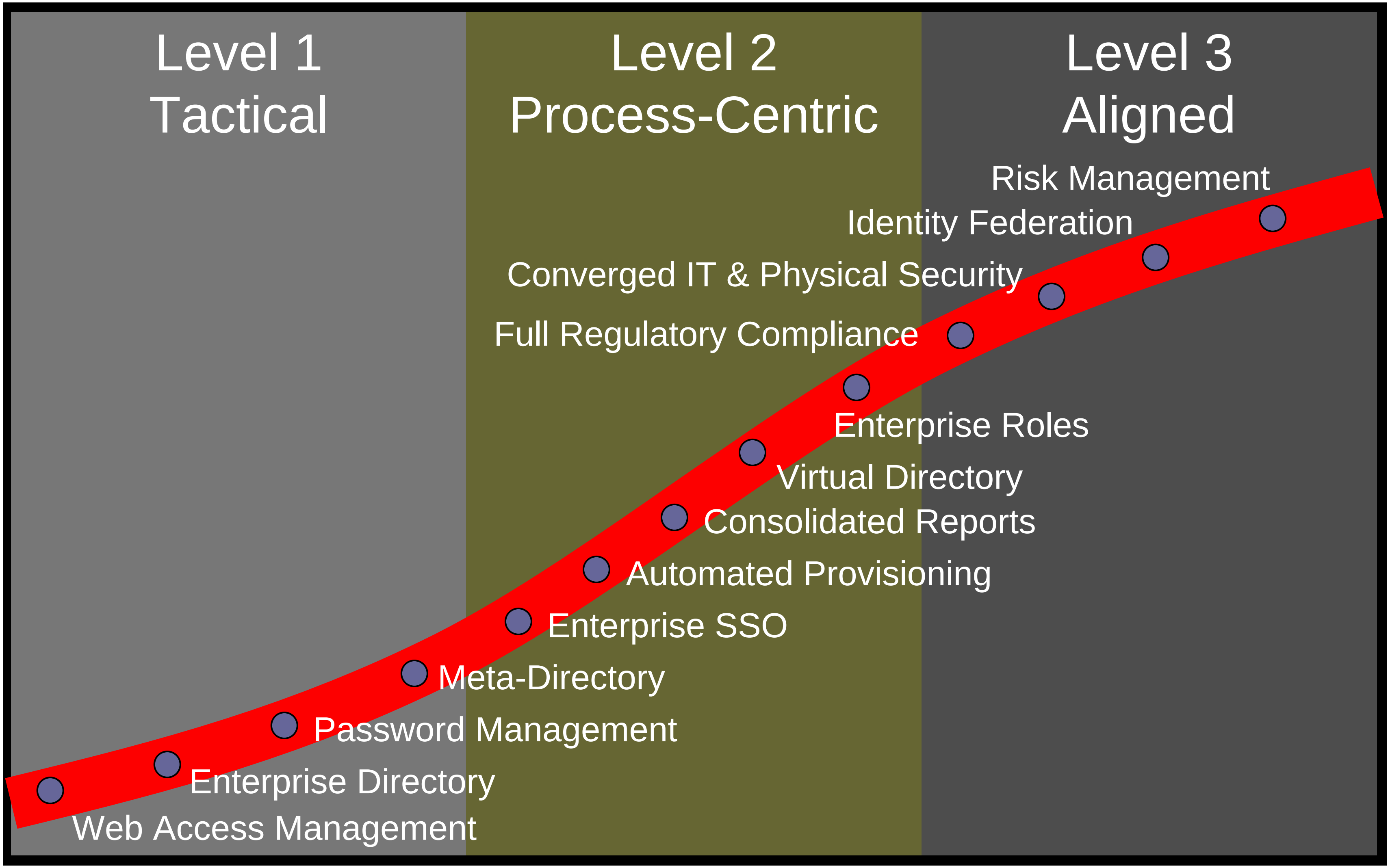
Continue the Dialogue On My Blog

http://www.talkingidentity.com

Appendix: Get Involved!

- Project Concordia
  - http://projectconcordia.org/index.php/Main_Page
- Internet Identity Workshop
  - http://iiw.windley.com/
- Liberty Alliance
  - http://www.projectliberty.org/
- Burton Group's Identity Services Working Group

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