Security, Risk and Compliance

Soluzioni IBM Tivoli per l'Identity e l’Access Management

Casi Reali di Implementazione

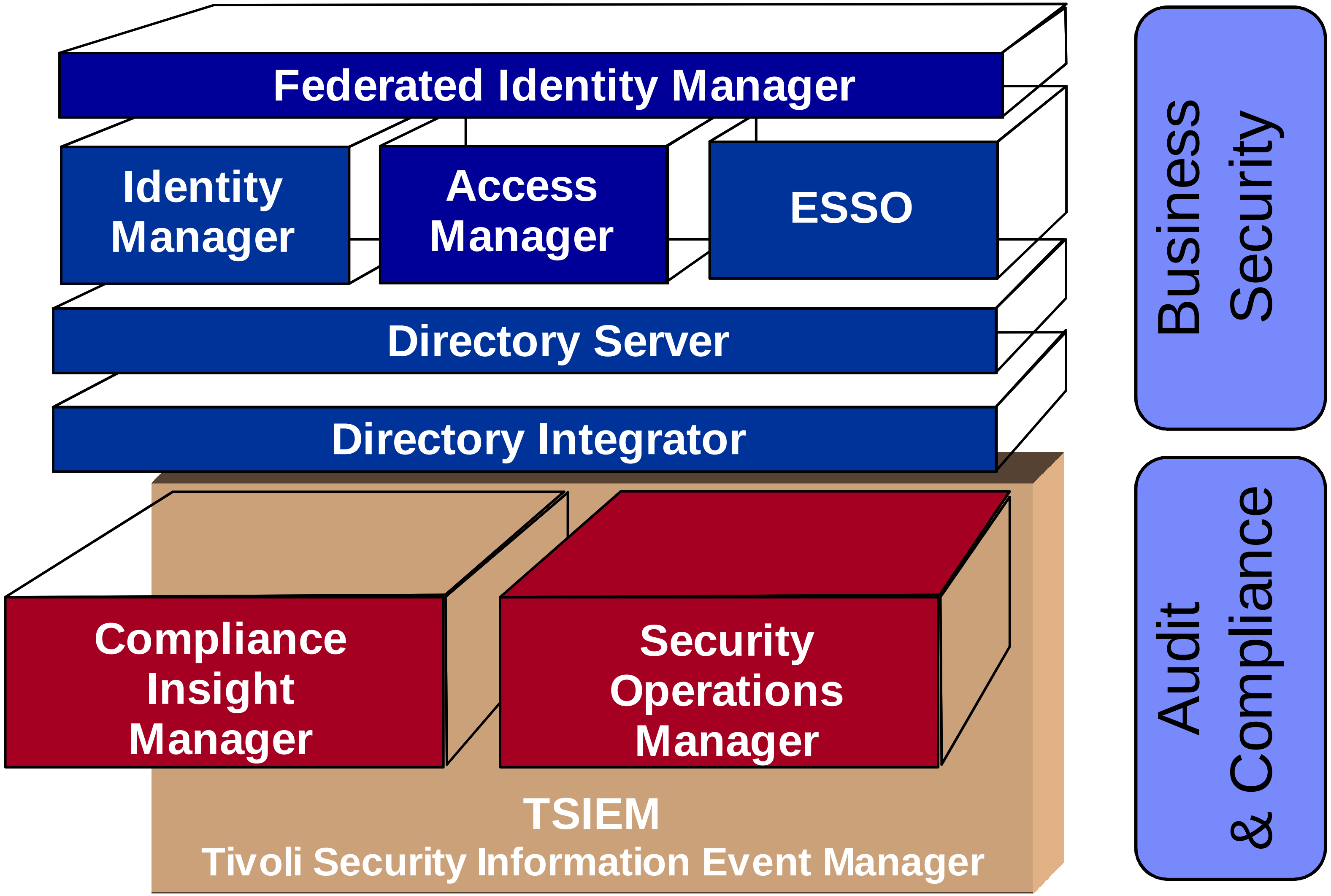
Alessandro Faustini
Technical Sales Specialist – Tivoli Security
IBM Italia S.p.A.

IBM Service Management World Tour & Tivoli User Group

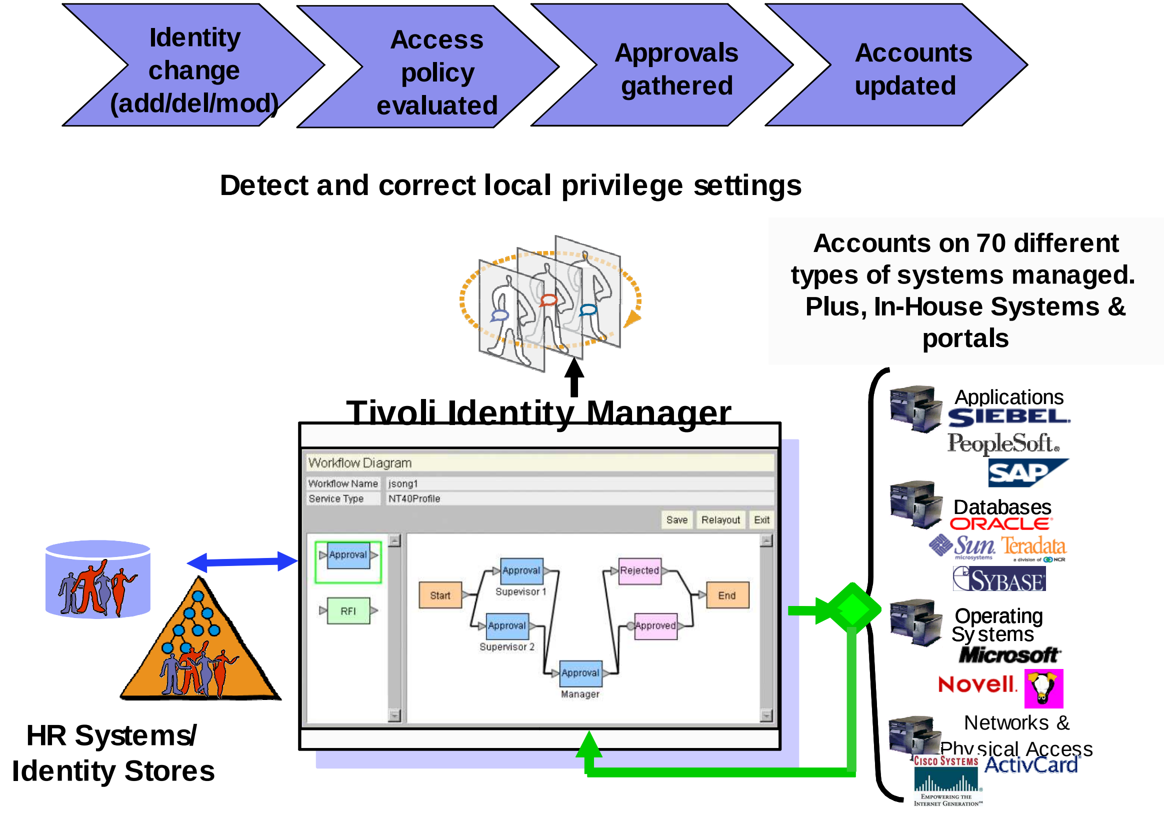
Roma, 20 ottobre 2008

Identity & Access Management

Manage users, identities, access rights, enforce & monitor user activity on all IT systems


Federated Identity Manager
Identity Manager
Access Manager
ESSO
Directory Server
Directory Integrator
Compliance Insight Manager
Security Operations Manager
TSIEM
Tivoli Security Information Event Manager
Business Security
Audit & Compliance

Tivoli Identity Manager automates, audits, and manages user access rights across your IT infrastructure



Identity change (add/del/mod)

Access policy evaluated

Approvals gathered

Accounts updated

Detect and correct local privilege settings

Accounts on 70 different types of systems managed. Plus, In-House Systems & portals

Tivoli Identity Manager

Workflow Diagram

Workflow Name: jsong1

Service Type: NT40Profile

HR Systems/ Identity Stores

- Know the ***people*** behind the accounts and ***why*** they have the access they do
- Fix non-compliant accounts
- Automate user privileges lifecycle across entire IT infrastructure
- Match your workflow processes

Simplify Complexity

- Business-relevant view of security
- Access rights audit & reports

Address Compliance

- Onboarding & recertification workflows
- Closed-loop provisioning

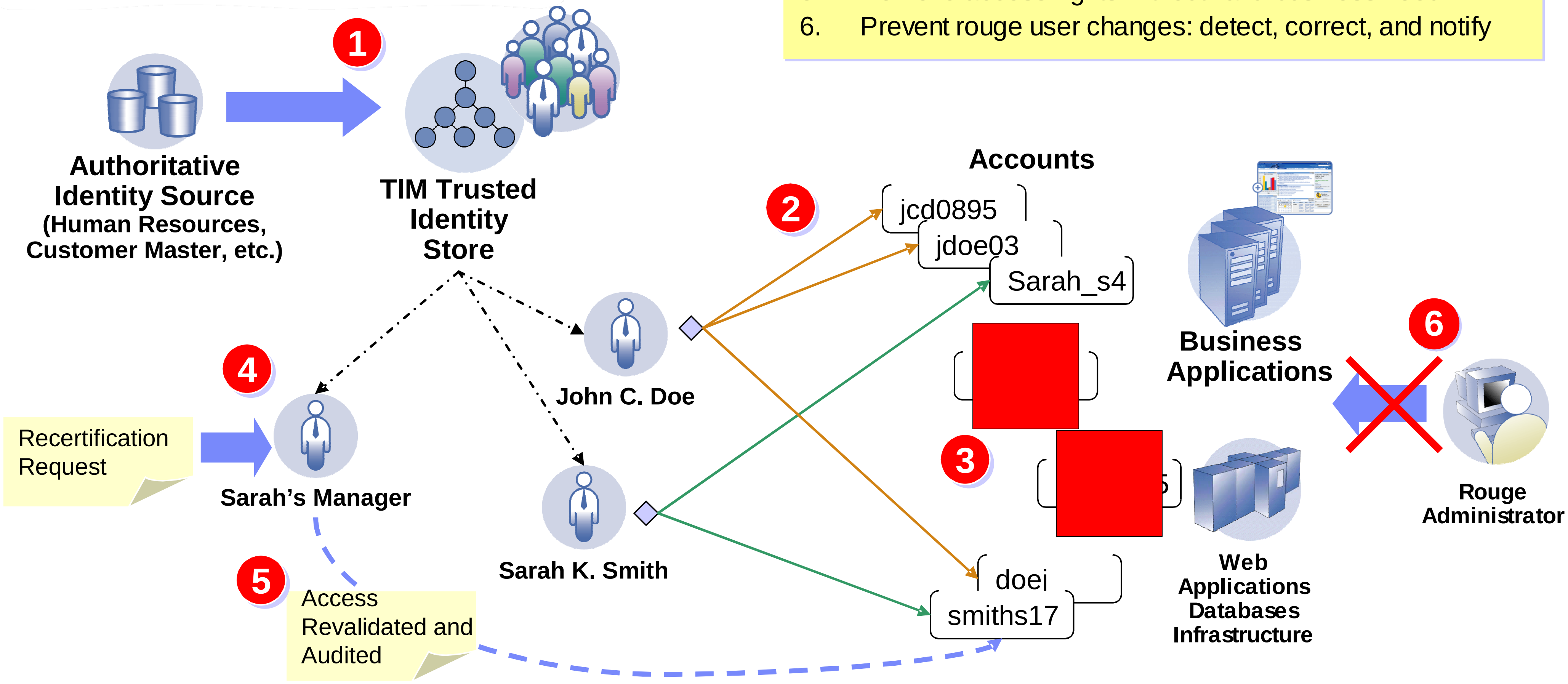
Reduce Costs

- Self-service password reset
- Automated user provisioning & de-provisioning

Improve security and compliance readiness through TIM automated security policy enforcement, audit, and reporting

30% or more of all accounts are 'orphans'
Gartner Group

1. Know the users, understand business context
2. Match accounts to real people
3. Eliminate rouge or 'orphan' accounts
4. Management review and attestation of user rights
5. Remove access rights without valid business need
6. Prevent rouge user changes: detect, correct, and notify



1

Authoritative Identity Source
(Human Resources, Customer Master, etc.)

TIM Trusted Identity Store

2

Accounts

jcd0895

jdoe03

Sarah_s4

[redacted]

[redacted]

doei

smiths17

3

John C. Doe

Sarah K. Smith

4

Recertification Request

Sarah's Manager

5

Access Revalidated and Audited

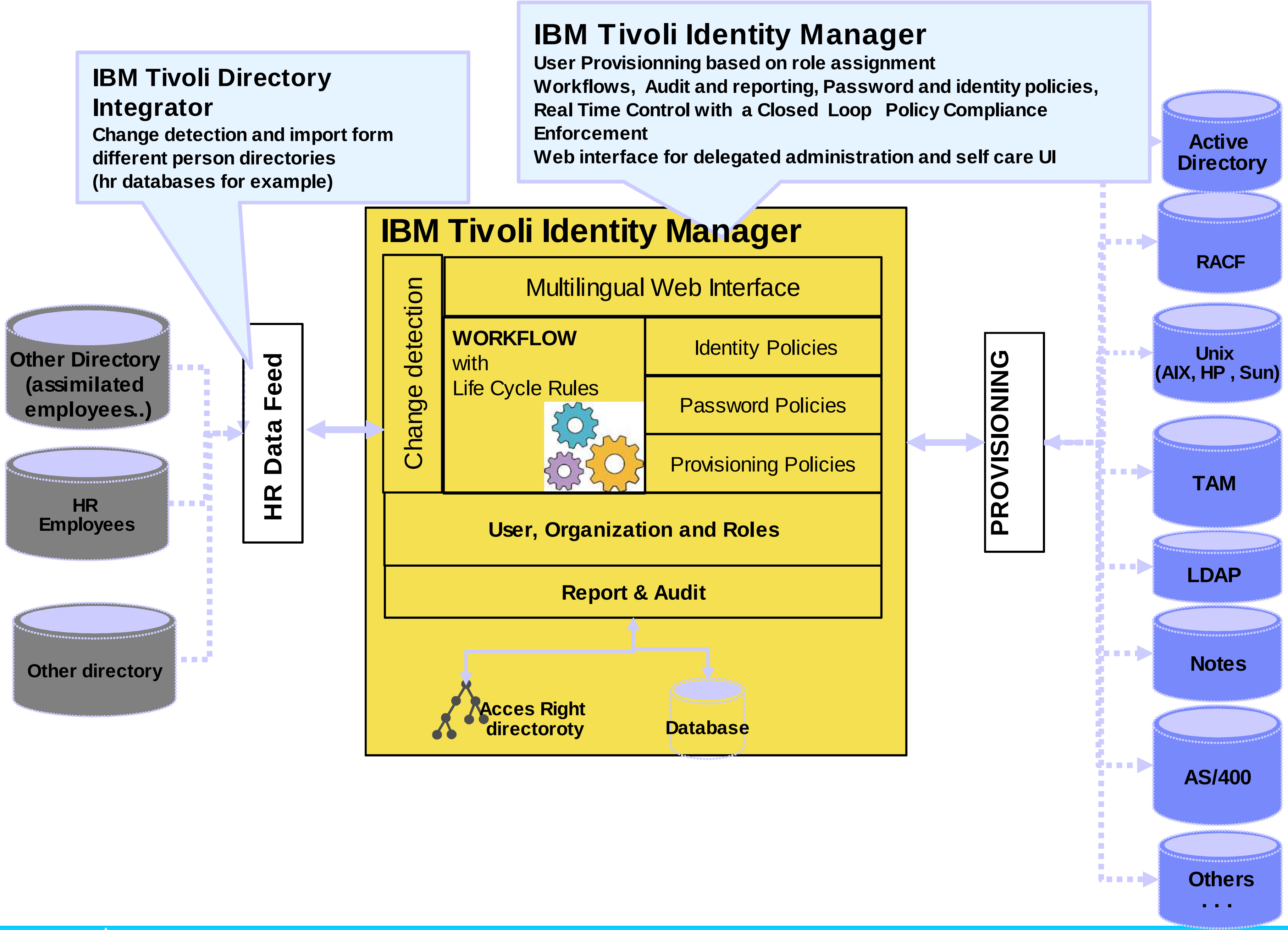
Business Applications

Web Applications Databases Infrastructure

6

Rouge Administrator

Tivoli Identity Manager: Logical Architecture



IBM Tivoli Directory Integrator

Change detection and import form different person directories (hr databases for example)

IBM Tivoli Identity Manager

User Provisionning based on role assignment

Workflows, Audit and reporting, Password and identity policies,

Real Time Control with a Closed Loop Policy Compliance Enforcement

Web interface for delegated administration and self care UI

Other Directory (assimilated employees..)

HR Employees

Other directory

HR Data Feed

IBM Tivoli Identity Manager

Change detection

Multilingual Web Interface

WORKFLOW with Life Cycle Rules

Identity Policies

Password Policies

Provisioning Policies

User, Organization and Roles

Report & Audit

Acces Right directoroty

Database

PROVISIONING

Active Directory

RACF

Unix (AIX, HP , Sun)

TAM

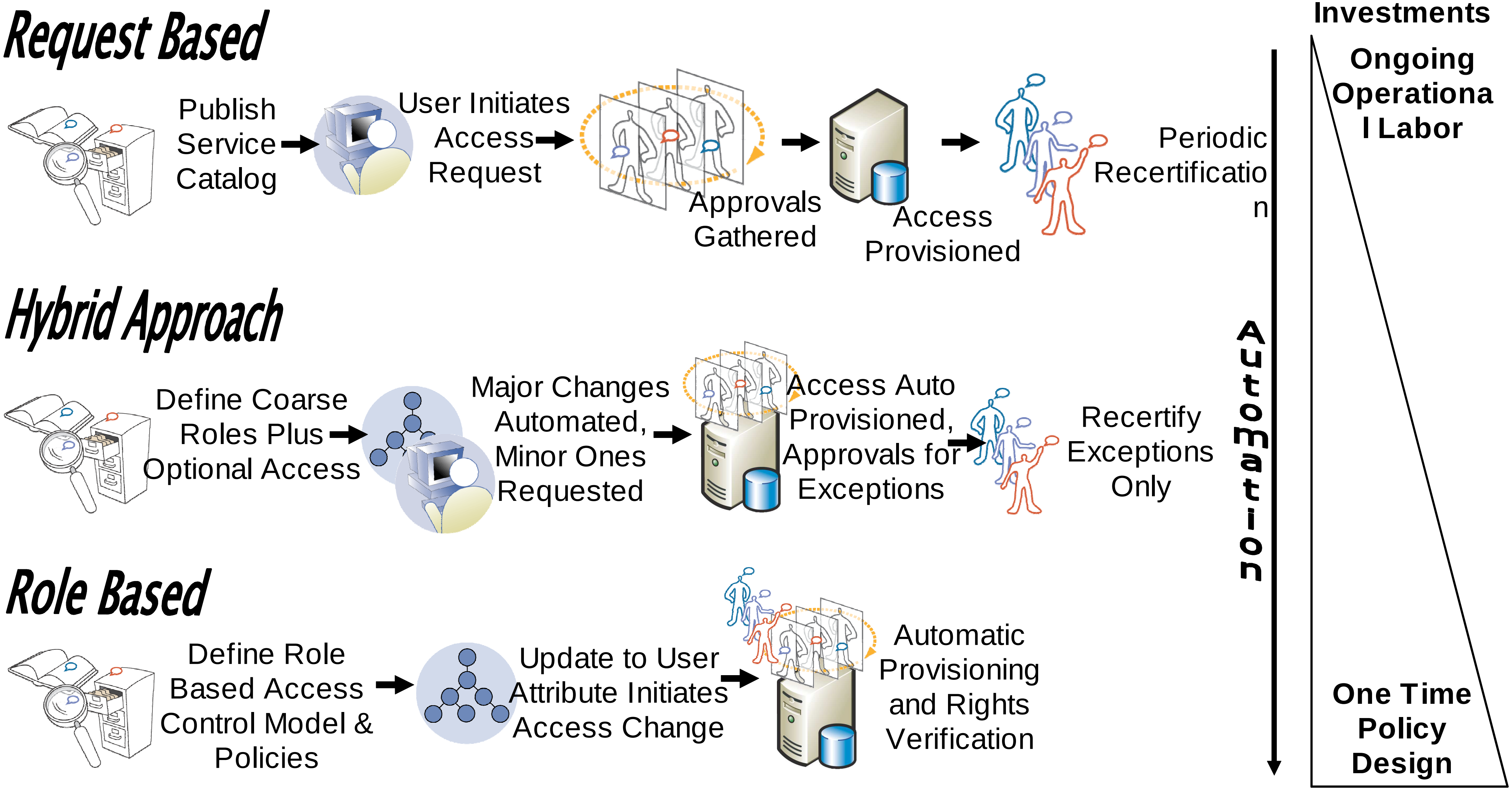
LDAP

Notes

AS/400

Others . . .

A phased approach to automating user provisioning with TIM delivers increasing improvements in efficiency and control



Request Based

Publish Service Catalog → User Initiates Access Request → Approvals Gathered → Access Provisioned → Periodic Recertificatio n

Hybrid Approach

Define Coarse Roles Plus Optional Access → Major Changes Automated, Minor Ones Requested → Access Auto Provisioned, Approvals for Exceptions → Recertify Exceptions Only

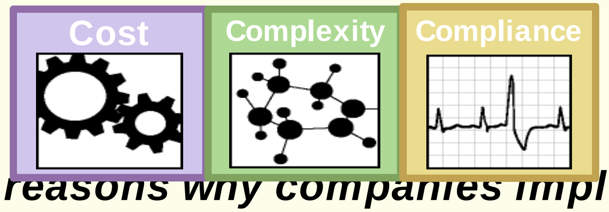
Role Based

Define Role Based Access Control Model & Policies → Update to User Attribute Initiates Access Change → Automatic Provisioning and Rights Verification

Why Role Management?

Why are companies looking at Roles?

- **Provide efficiencies in administration**
- **Address security risks (least privilege)**
- **Demonstrate compliance**



Same reasons why companies implement Identity Management systems

What is Role Management?

The Process

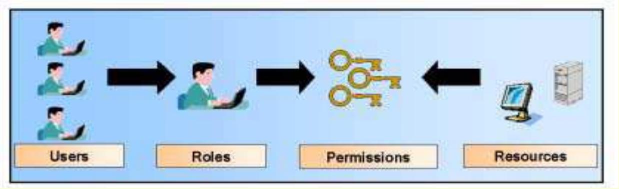
- **Defining – mining, modeling**
- **Creating – discover, design**
- **Maintaining – role lifecycle**
- **Managing – who has access to what**

Must address the needs of both ***business*** **and** ***technical*** **users**

What are Roles?

Roles define permissions which are composed of objects and operations. Users obtain access to resources (objects) through role assignments

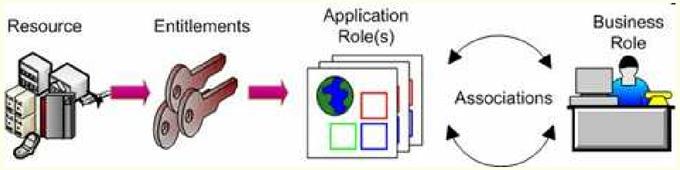
RBAC is the model for controlling access to resources based on roles rather than individual assignments



Types of Roles

Technical Roles – IT roles, resources roles, applications roles, system roles (bottom up)

Business Roles – Organization roles, Job roles, Functional roles, Process roles, Project roles (top down)

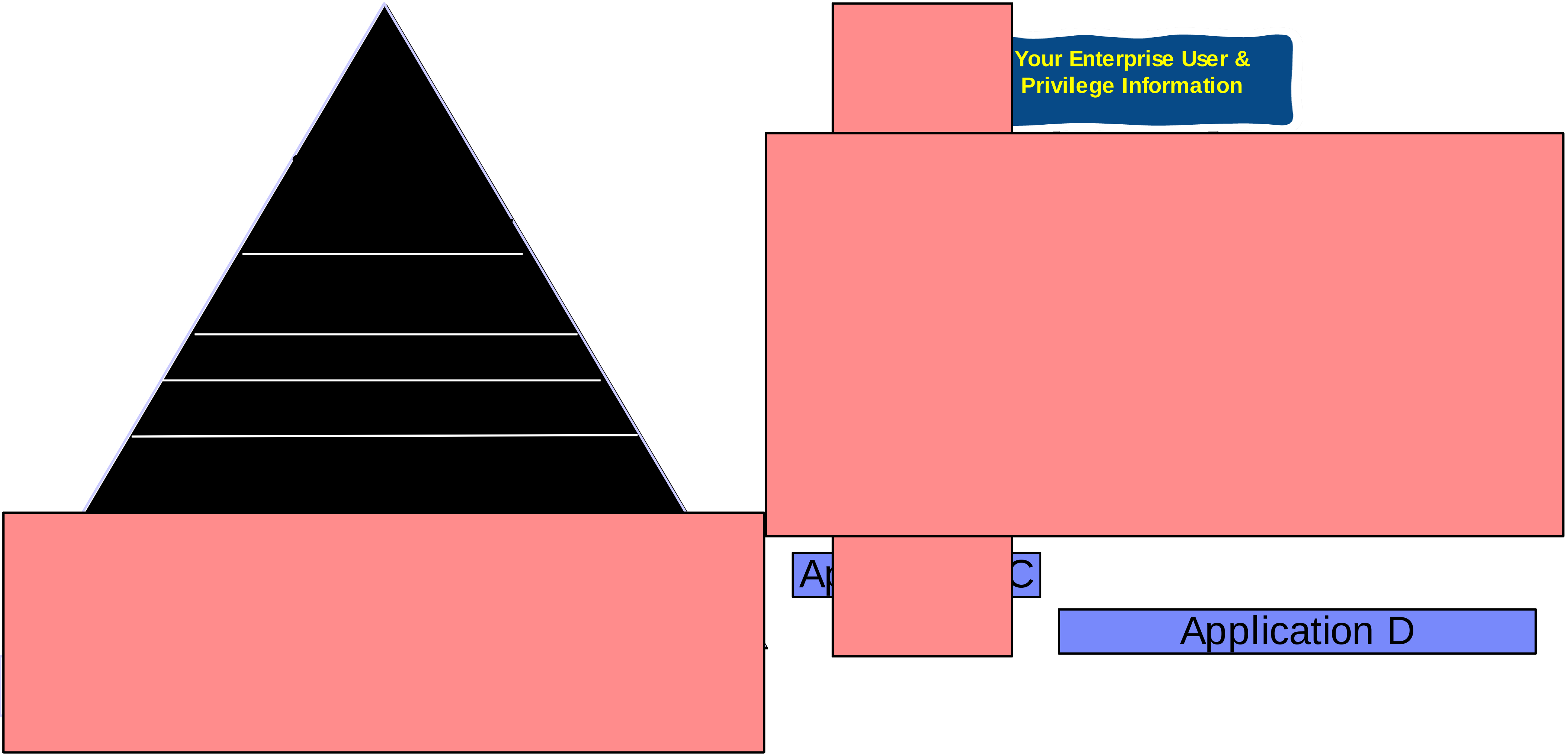


Role Lifecycle Management Processes

	Process Details
Plan	**Establish business goals/objectives for role management project (i.e. enhanced security, compliance, reduction in administrative costs)**
	Secure line management approvals and executive sponsorship to ensure consistent oversight and continued prioritization
Collect	**Identify and communicate with LOB personnel who will provide background on current business roles and business processes.**
	Identify and collect data from target systems that have relevant user and entitlement data. Start construction of role/entitlement catalog
Analyze	**Analyze information collected on business roles - validate and clarify any inconsistencies with LOB personnel**
	Evaluate common sets of authorizations for entitlement data
Engineering	**Define roles – create business role definitions that align to the job functions within the company and the application role definitions that represent common sets of authorizations across the infrastructure**
	Map business roles to application roles (based on common sets of authorizations)
	Define role hierarchy – establish the relevant parent and child business roles (inheritance is intrinsic)
	Define Separation of Duty policies – define conflicts that exist at business role (accts payable/accts receivable) and at application role (funds disbursement/invoicing)
Verify	**Simulate what-if scenarios to test business and application roles created, make necessary adjustments**
	Establish role and provisioning policy definition approvals and recertification workflows
Administer	**Assign business role ownership and application role ownership – who is actually going to be responsible for the role definitions?**
	Determine business role membership – who belongs to what roles?
	Create/modify provisioning policies with new role structure – provisioning of entitlements through application roles
	Establish recertification policies for role membership, user accounts, and access entitlements/groups
	Import and/or migrate users into their business roles
	If need exists for requesting roles, establish rules for role, user account and access entitlement approvals
	Ongoing administration and change control
Report	**Issue reports on business roles, application roles and entitlements**
	Any metrics/learnings gained in process should be fed back in to role management system and be utilized for additional governance

Deployments can be staged by functionality delivered, organisation served, or systems managed

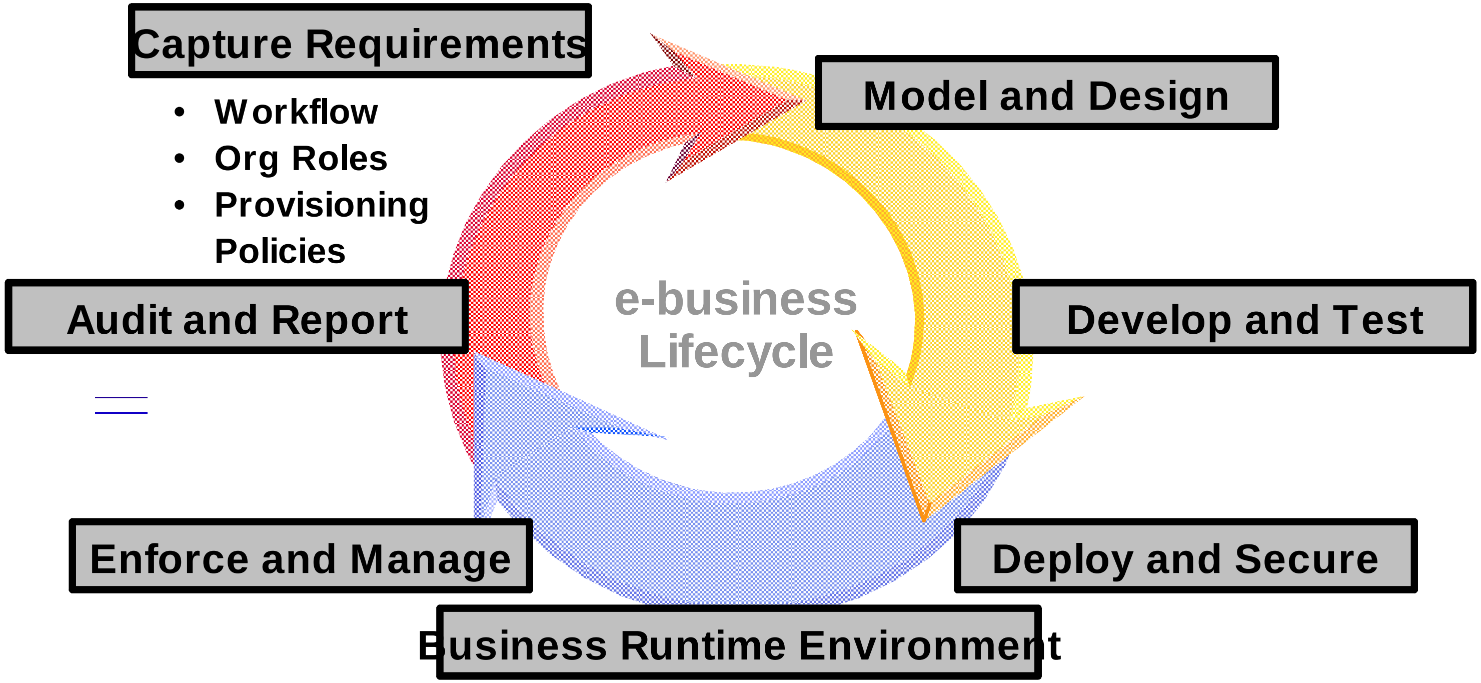
Flexible



Who Does What and When? – Implementation

<table>
<tr><th colspan="2"></th><th>PREPARATION and PLANNING</th><th>FRAMEWORK</th><th>DESIGN</th><th>CONFIGURATION</th><th>DEPLOY TO PRODUCTION</th></tr>
<tr><td colspan="2" rowspan="3">Project Mgmt.</td><td>Determine Scope and Approach</td><td colspan="4">Budget and Actuals Tracking</td></tr>
<tr><td>Document As-Is Process Maps</td><td colspan="3">Develop and Maintain Work Plan</td><td>Project Wrap-up Activities</td></tr>
<tr><td>Perform Readiness Assessment</td><td colspan="4">Monitoring and Reporting Activities</td></tr>
<tr><td colspan="2">Tech Ed</td><td>Schedule Training</td><td>Project Team Training</td><td>Administrator Training</td><td>Help Desk Support Training</td><td>End User Training</td></tr>
<tr><td colspan="2" rowspan="3">Technical Installation</td><td rowspan="2">Technology Architecture Drawing and Solution Design</td><td>Install and Test E/S</td><td colspan="3">Document Installation History</td></tr>
<tr><td>Install and Test Adapters</td><td colspan="3">Perform System Tuning</td></tr>
<tr><td>Verify Client Environment</td><td>Data File Design</td><td>Data Files Preparation</td><td colspan="2">Data Loading</td></tr>
<tr><td rowspan="5">Implementation</td><td>Org/ Conf</td><td></td><td>Configure Organisation Structure and Roles</td><td>Design Account Management Forms</td><td colspan="2">Configure Account Management Forms</td></tr>
<tr><td>Grp/ ACI</td><td></td><td colspan="2">Design ITIM Groups and ACIs</td><td colspan="2">Configure ITIM Groups and ACIs</td></tr>
<tr><td>Policy</td><td></td><td colspan="2">Develop Provisioning Policies and Entitlements</td><td colspan="2">Configure Provisioning Policies and Entitlements</td></tr>
<tr><td>Work-Flow</td><td></td><td>Develop To-Be Process Maps</td><td>Design Security Administration Workflows & Procedures</td><td>Configure Security Administration Workflows & Procedures</td><td>Enable Chosen Workflows and Procedures</td></tr>
<tr><td>Auto</td><td></td><td>Develop Automated Processes</td><td>Design Testing Strategy and Scripts</td><td>Perform Pre-Production Testing</td><td>Reconciliation and Orphan Account Cleanup</td></tr>
</table>

IAM Project execution lifecycle



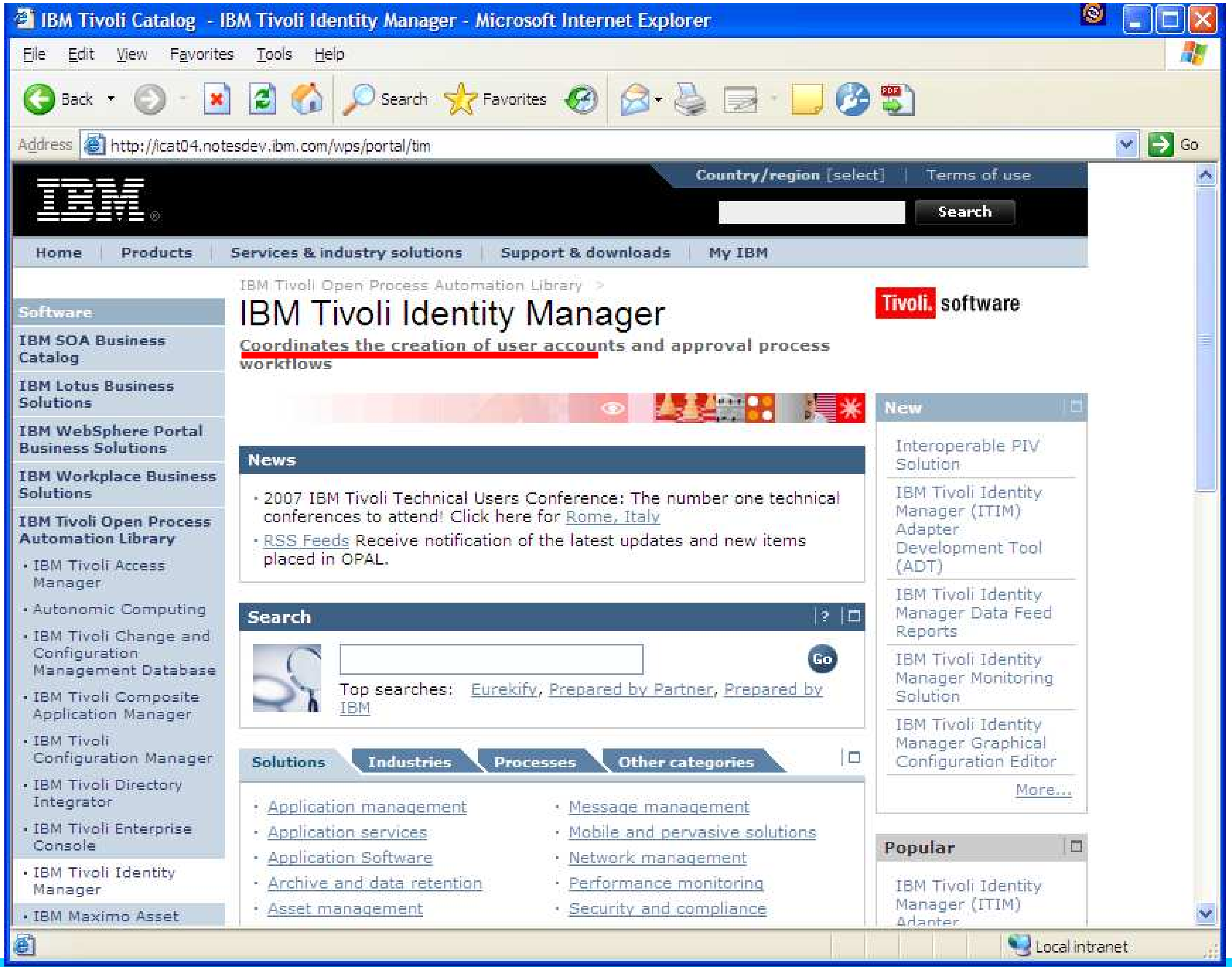
Continuous Deployment Cycle by:

- Line of Business, or
- Platform, or
- Application

Open Process Automation Library

- http://catalog.lotus.com/wps/portal/topal

- A comprehensive online catalog of IBM Tivoli product extensions from IBM and from our partners including automation packages, integration adapters, agents, documentation and supporting information.


IBM Tivoli Catalog - IBM Tivoli Identity Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://icat04.notesdev.ibm.com/wps/portal/tim
Go
Country/region [select] | Terms of use
Search
Home | Products | Services & industry solutions | Support & downloads | My IBM
Tivoli. software
Local intranet

Software

IBM SOA Business Catalog

IBM Lotus Business Solutions

IBM WebSphere Portal Business Solutions

IBM Workplace Business Solutions

IBM Tivoli Open Process Automation Library

- IBM Tivoli Access Manager
- Autonomic Computing
- IBM Tivoli Change and Configuration Management Database
- IBM Tivoli Composite Application Manager
- IBM Tivoli Configuration Manager
- IBM Tivoli Directory Integrator
- IBM Tivoli Enterprise Console
- IBM Tivoli Identity Manager
- IBM Maximo Asset

IBM Tivoli Open Process Automation Library >

IBM Tivoli Identity Manager

Coordinates the creation of user accounts and approval process workflows

News

- 2007 IBM Tivoli Technical Users Conference: The number one technical conferences to attend! Click here for Rome, Italy
- RSS Feeds Receive notification of the latest updates and new items placed in OPAL.

Search

Go

Top searches: Eurekify, Prepared by Partner, Prepared by IBM

Solutions | Industries | Processes | Other categories

- Application management
- Application services
- Application Software
- Archive and data retention
- Asset management
- Message management
- Mobile and pervasive solutions
- Network management
- Performance monitoring
- Security and compliance

New

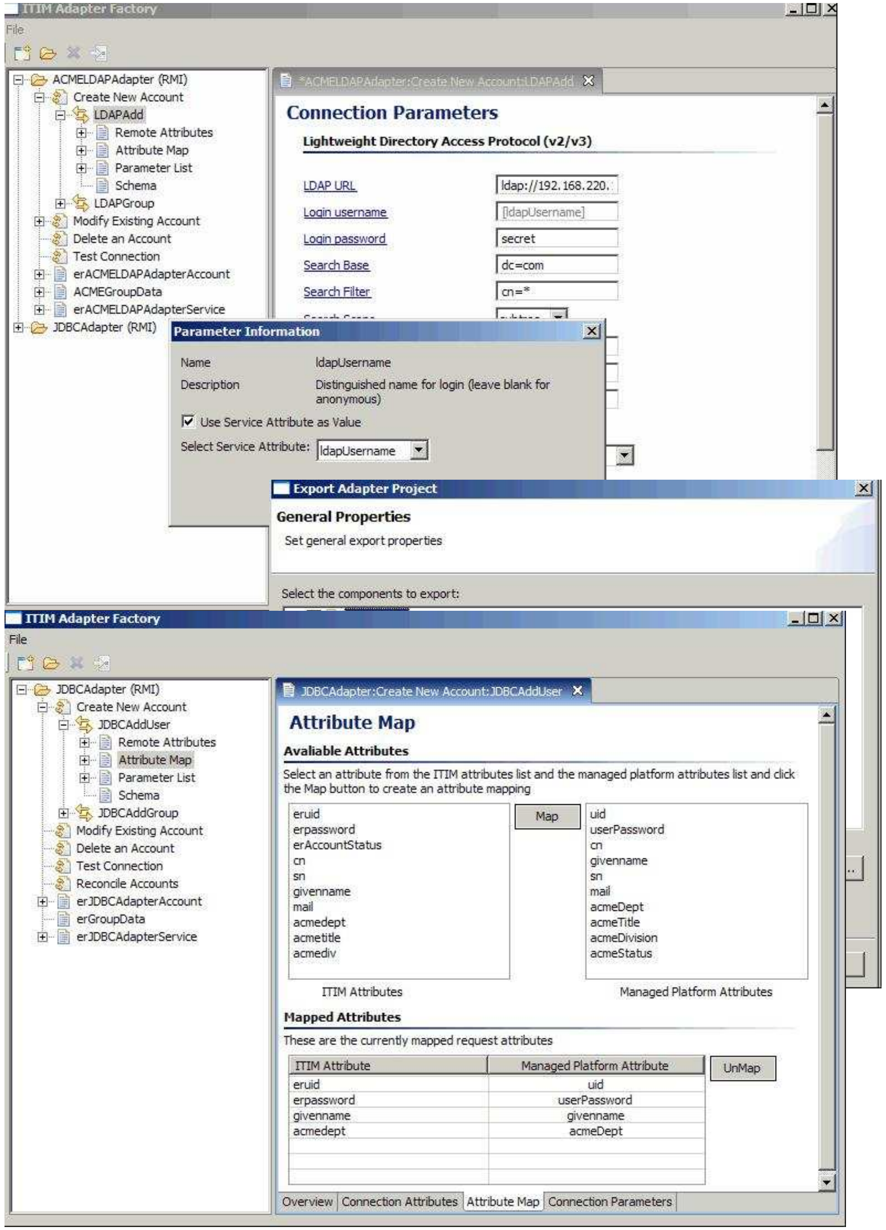
- Interoperable PIV Solution
- IBM Tivoli Identity Manager (ITIM) Adapter Development Tool (ADT)
- IBM Tivoli Identity Manager Data Feed Reports
- IBM Tivoli Identity Manager Monitoring Solution
- IBM Tivoli Identity Manager Graphical Configuration Editor

More...

Popular

- IBM Tivoli Identity Manager (ITIM) Adapter

Easily Integrate with Homegrown and Niche Applications


ITIM Adapter Factory

File

- ACMELDAPAdapter (RMI)
  - Create New Account
    - LDAPAdd
      - Remote Attributes
      - Attribute Map
      - Parameter List
      - Schema
    - LDAPGroup
  - Modify Existing Account
  - Delete an Account
  - Test Connection
  - erACMELDAPAdapterAccount
  - ACMEGroupData
  - erACMELDAPAdapterService
- JDBCAdapter (RMI)

*ACMELDAPAdapter:Create New Account:LDAPAdd

Connection Parameters

Lightweight Directory Access Protocol (v2/v3)

LDAP URL: ldap://192.168.220.

Login username: [ldapUsername]

Login password: secret

Search Base: dc=com

Search Filter: cn=*

Parameter Information

Name: ldapUsername

Description: Distinguished name for login (leave blank for anonymous)

☑ Use Service Attribute as Value

Select Service Attribute: ldapUsername

Export Adapter Project

General Properties

Set general export properties

Select the components to export:

ITIM Adapter Factory

File

- JDBCAdapter (RMI)
  - Create New Account
    - JDBCAddUser
      - Remote Attributes
      - Attribute Map
      - Parameter List
      - Schema
    - JDBCAddGroup
  - Modify Existing Account
  - Delete an Account
  - Test Connection
  - Reconcile Accounts
  - erJDBCAdapterAccount
  - erGroupData
  - erJDBCAdapterService

JDBCAdapter:Create New Account:JDBCAddUser

Attribute Map

Avaliable Attributes

Select an attribute from the ITIM attributes list and the managed platform attributes list and click the Map button to create an attribute mapping

ITIM Attributes: eruid, erpassword, erAccountStatus, cn, sn, givenname, mail, acmedept, acmetitle, acmediv

Managed Platform Attributes: uid, userPassword, cn, givenname, sn, mail, acmeDept, acmeTitle, acmeDivision, acmeStatus

Mapped Attributes

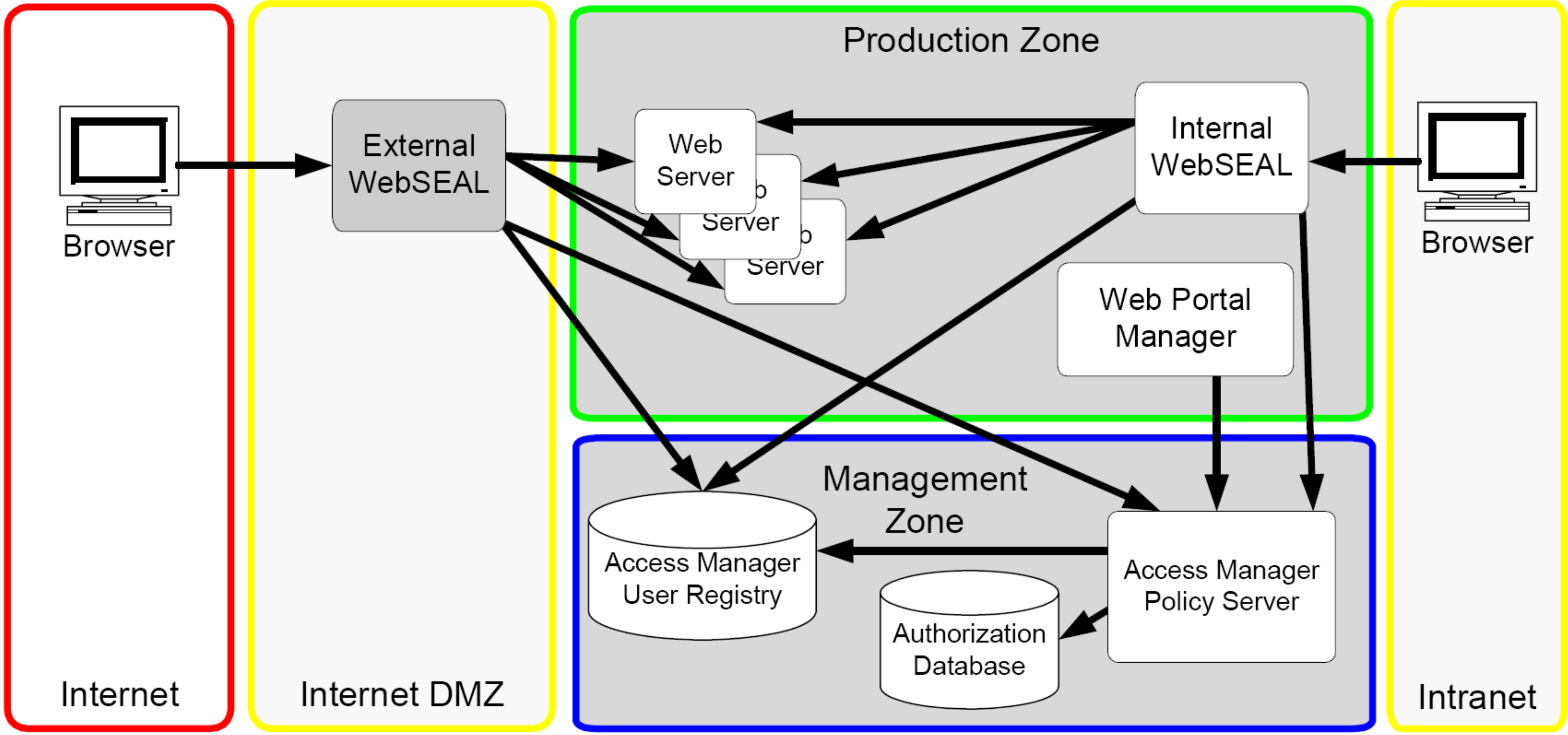
These are the currently mapped request attributes

ITIM Attribute	Managed Platform Attribute
eruid	uid
erpassword	userPassword
givenname	givenname
acmedept	acmeDept

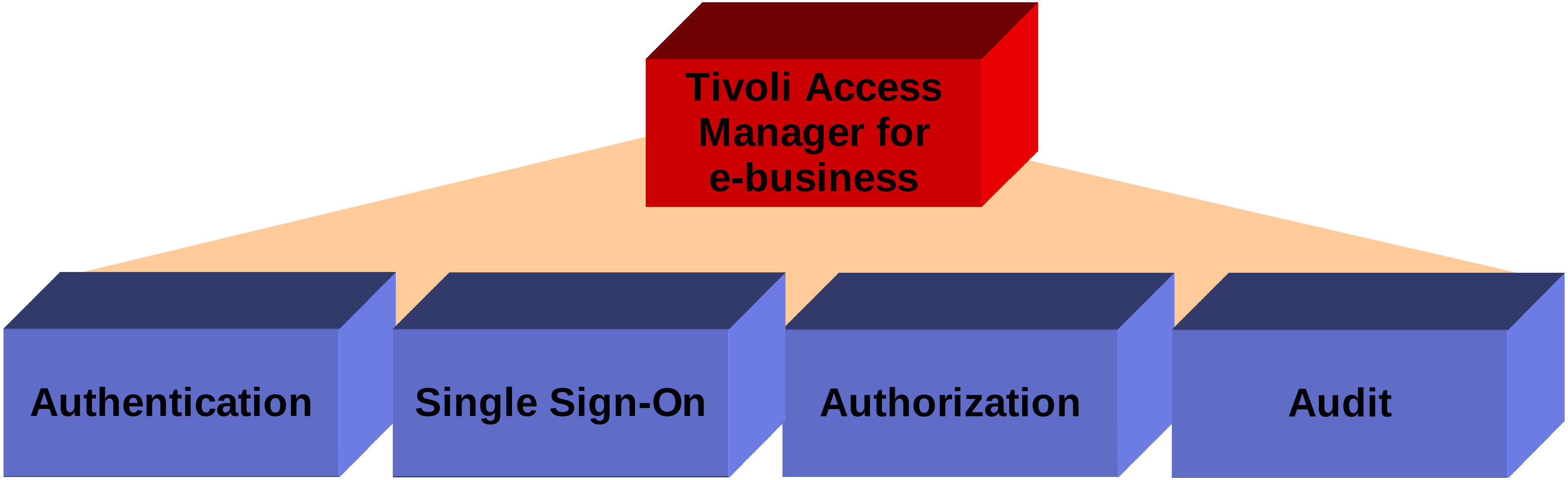
TIM Adapter Development Tool

- Effectively meet the need to integrate with any home grown applications
- Wizard based approach to quickly build custom TIM adapters
  - Select connector type and connect to the target system
  - Discover and map attributes to manage
  - Choose TIM operations and publish adapter to TIM
- Reduce development time by 75%
  - Requires fewer specialized skills
  - Based on Eclipse framework and leverages Tivoli Directory Integrator

Access Management – Architecture overview with Tivoli Access Manager for eBusiness



Tivoli Access Manager - Key Capability



Tivoli Access Manager for e-business

Authentication

Single Sign-On

Authorization

Audit

Authentication

- Flexible choice among diverse authentication mechanisms
- Step-up
- Forced re-authentication

Single Sign-On

- Native—Desktop and Web SSO
- Integrate w/TFIM for federated SSO
- Integrate w/partner products for client/ server SSO

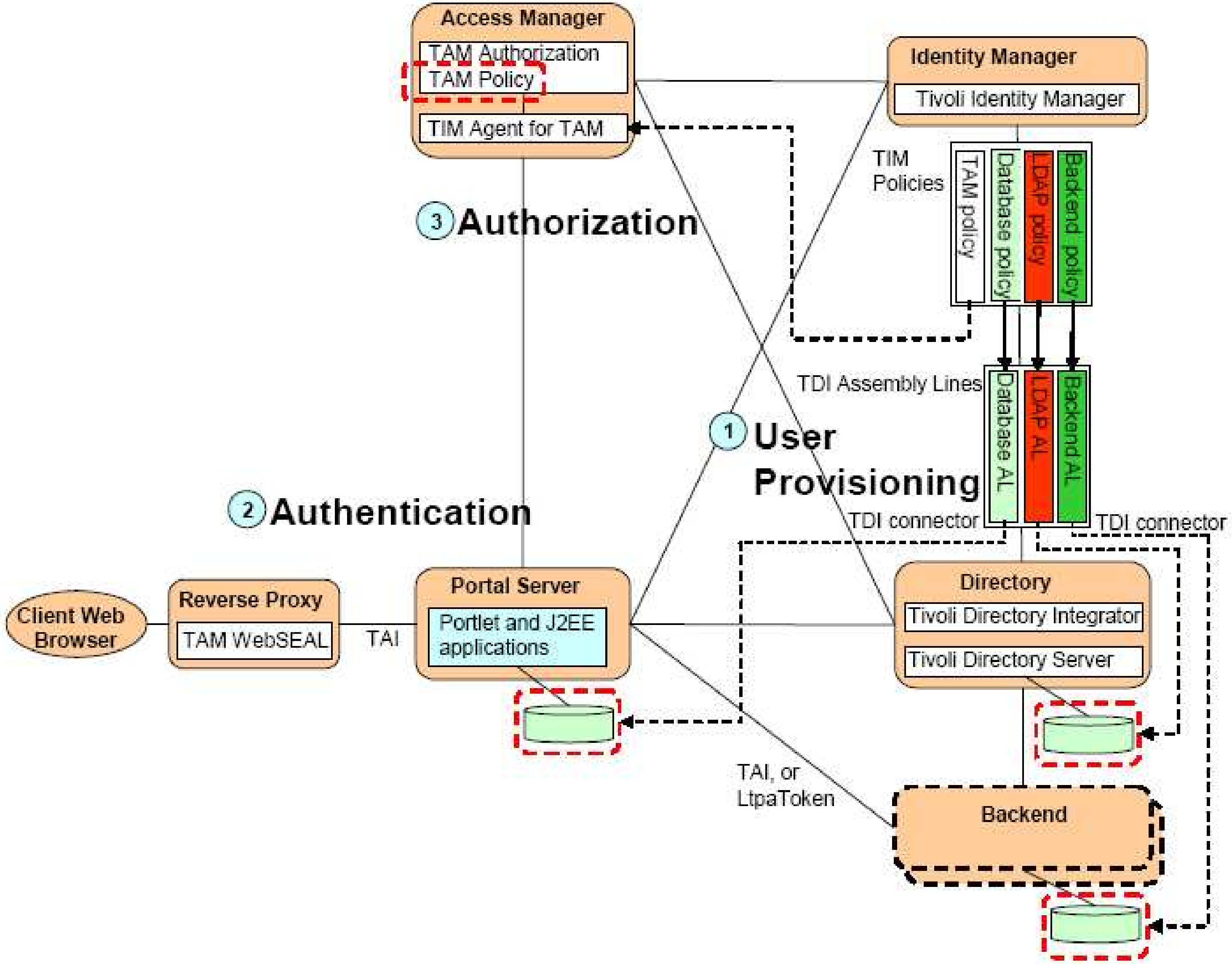
Authorization

- Policy-driven
- Resource "agnostic"
- Standards-based (Java, .NET, C/C++)

Audit

- Enterprise-class auditing
- Reporting
- Key element for compliance

Use Case: Identity & Access Management Solution



TAMESSO Alleviates Customer Challenges

Customer Challenges

- Poor user productivity
- Weak user password security
- Escalating Help Desk costs
- Insecure heterogeneous infrastructure that includes custom and legacy applications
- Inefficient user access log collection
- Difficulty managing security in a shared desktop environment

TAMESSO Value

- Automated ESSO to help enhance user productivity, improve security, implement and document compliance efforts, and reduce support costs
- Broad support for common applications and flexible toolkit to extend to applications across the enterprise
- Extensive integration with strong authentication form factors
- Centralized auditing and reporting for visibility into user access
- Controlled session management for shared desktops

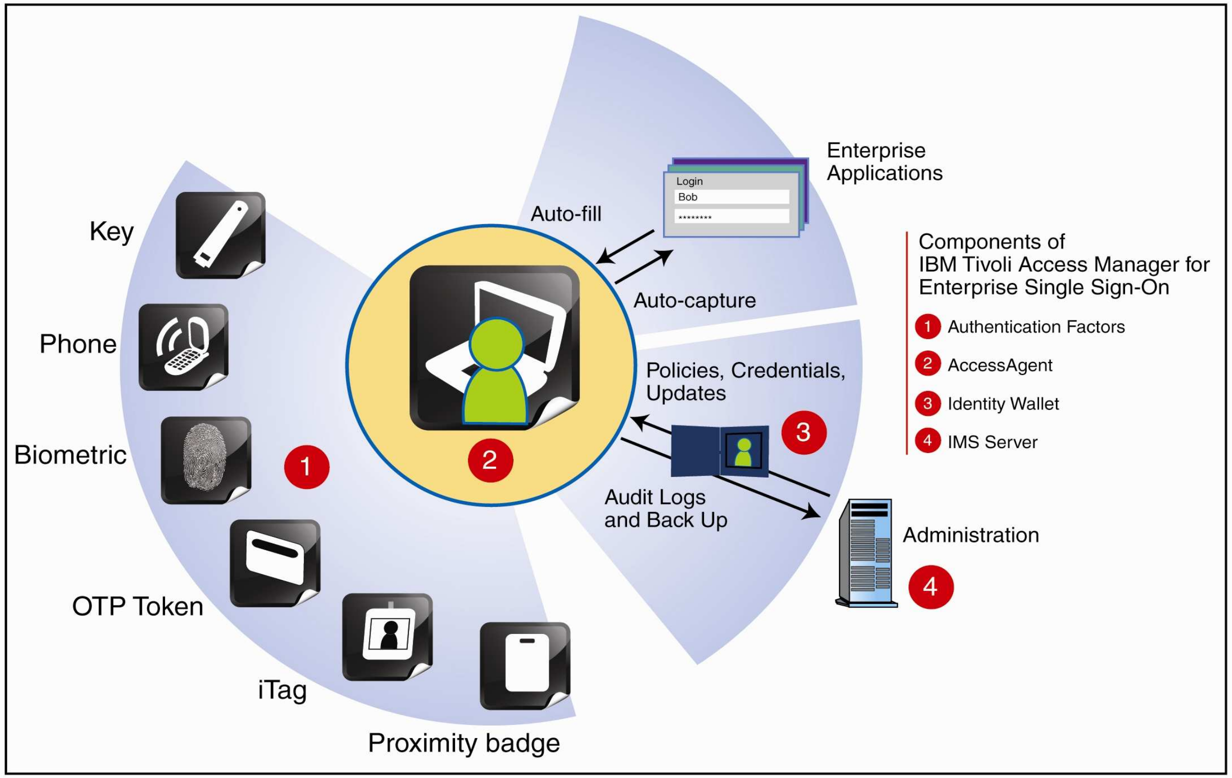
TAMESSO enables visibility into user activity, control over access to business assets, and automation of the sign-on process in order to drive value for our clients.

TAM ESSO v8 Solution Overview

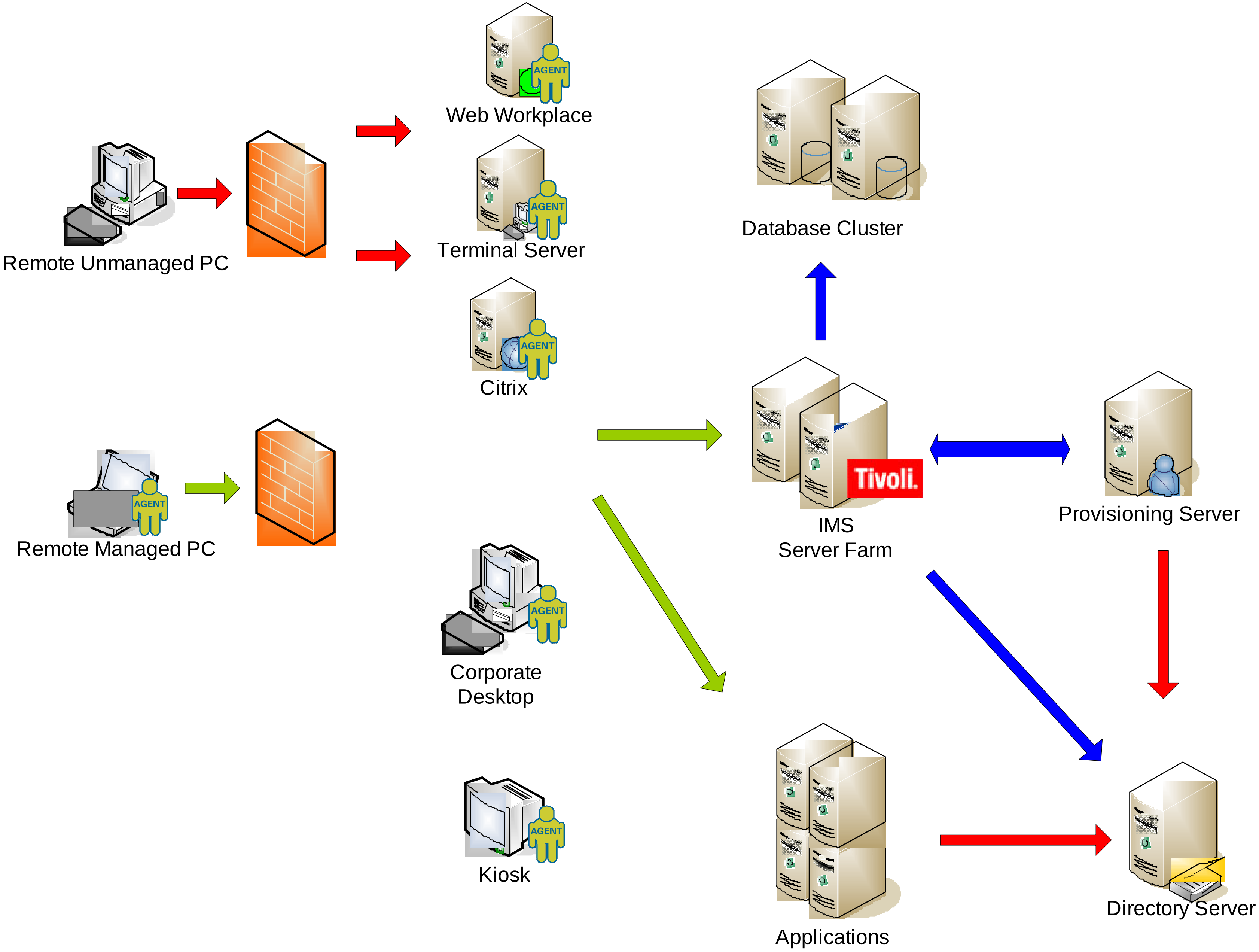
TAM ESSO provides:

- **ESSO**
- **Two-Factor Authentication**
- **Access and Security Workflow Automation**
- **Fast user switching**
- **User Access Tracking & Audit**
- **Centralized Identity & Policy Management**

with <u>no</u> change to the infrastructure



TAM ESSO v8 Architecture

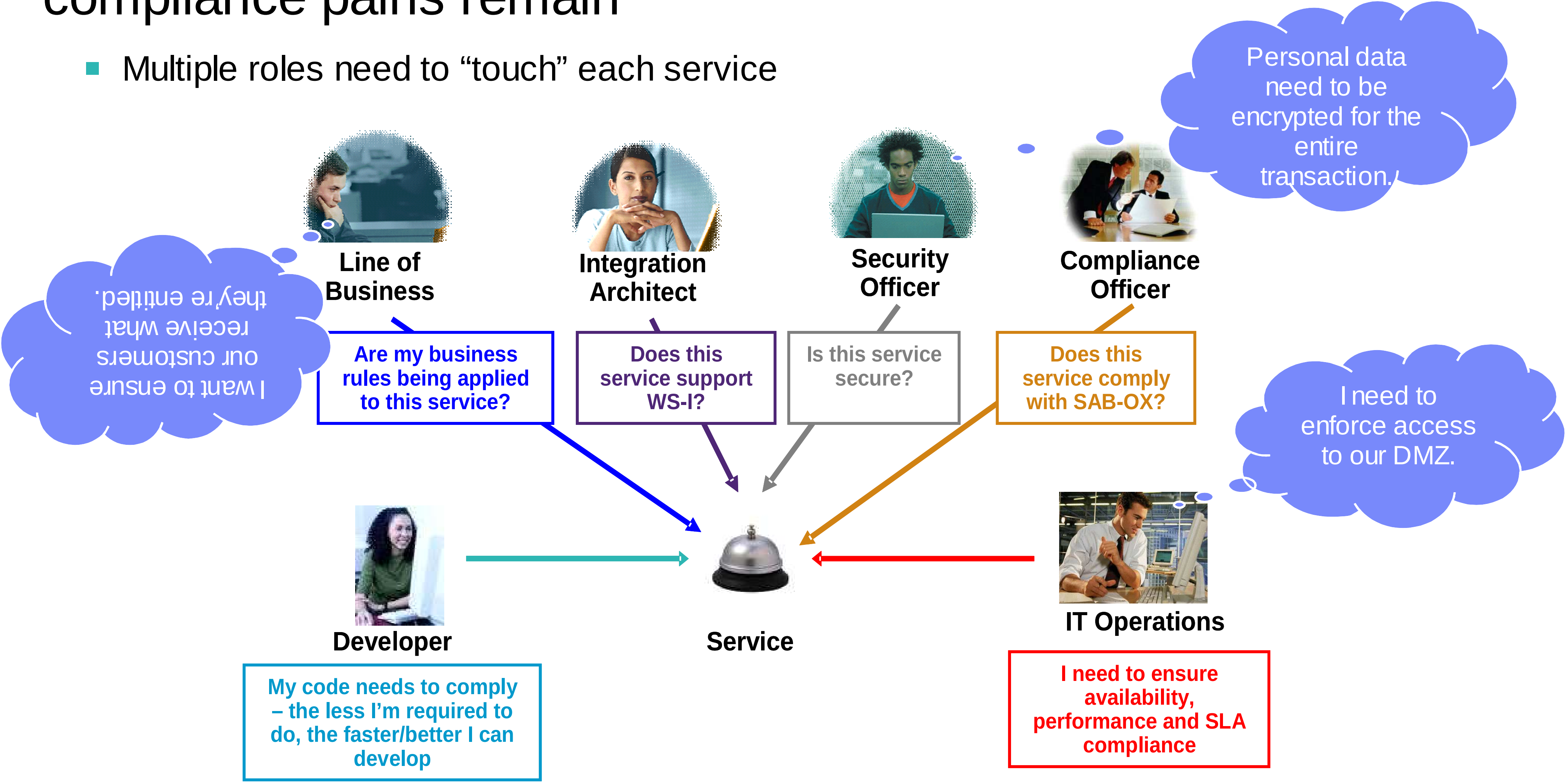


Companies are faced with new security management challenges as they move toward a service oriented architecture (SOA)

- **Composite application and mash-ups adoption**
  - Need consistent enforcement of policies
  - Requires enterprise to ensure consistent access control and data security
- **Compliance driving a need for closed-loop solution**
  - Need unified policy management with delegation & change control
  - Accountability and audit needs to relate activities to ‘end users’
- **Deployment of heterogeneous IT infrastructures creates costly islands of security administration**
  - Mature standards exist today (WS-Policy, WS-Trust, XACML)
  - Need common, pluggable framework (authentication, authorization)

Business flexibility has improved - but complexity and compliance pains remain

- Multiple roles need to “touch” each service



I want to ensure our customers receive what they’re entitled.

Line of Business

Are my business rules being applied to this service?

Integration Architect

Does this service support WS-I?

Security Officer

Is this service secure?

Compliance Officer

Does this service comply with SAB-OX?

Personal data need to be encrypted for the entire transaction.

I need to enforce access to our DMZ.

Developer

My code needs to comply – the less I’m required to do, the faster/better I can develop

Service

IT Operations

I need to ensure availability, performance and SLA compliance

Security Considerations in SOA

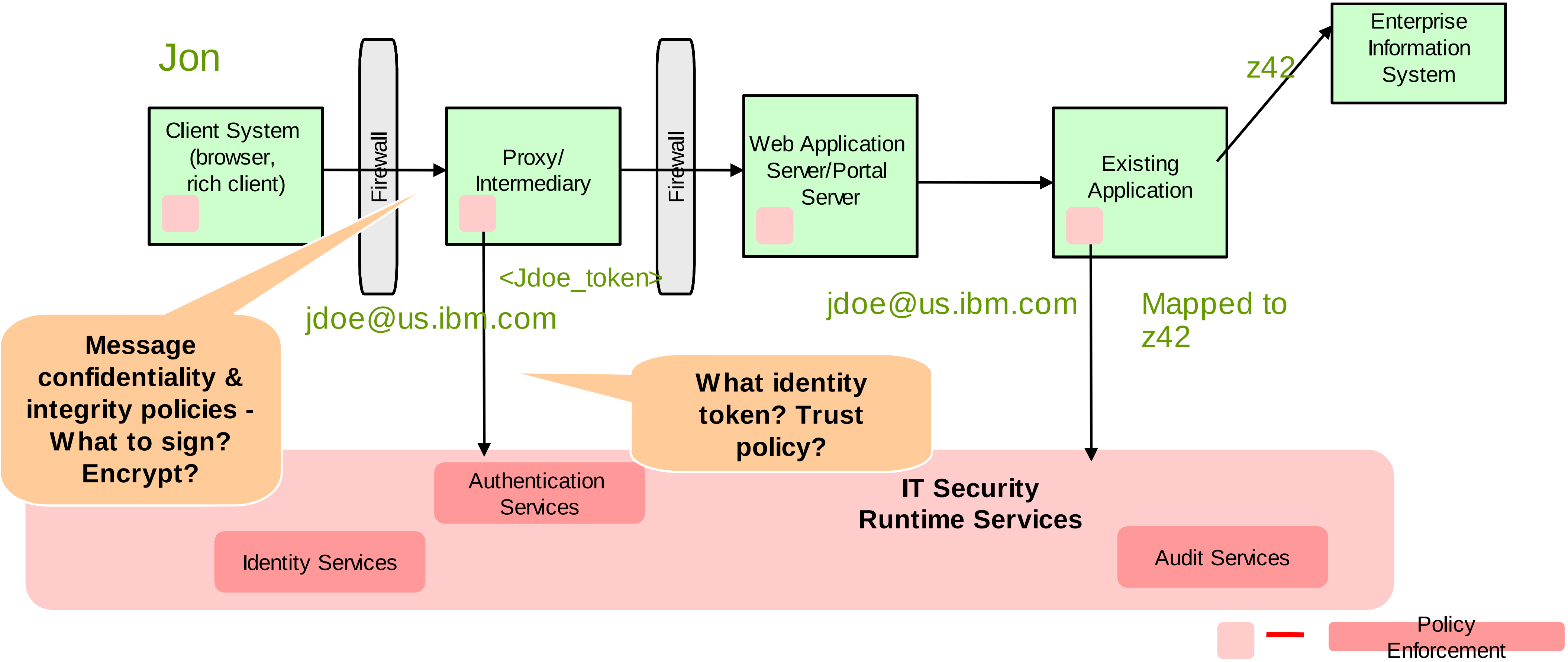
- Entities/Identities – users, services
  - Services have identities
  - Identities and/or credentials are propagated across services
- Organizational/enterprise boundaries
  - Perimeter is obscure
  - Identities and trust are managed across boundaries
- Composite applications
  - Ensuring proper security controls are enacted for each service and when used in combination
  - Consistent in security policy enforcement
- Greater focus on data/information
  - Protecting data at transit and at rest
  - Access to data by applications and services
- Governance, Risk, and Compliance
  - Audit and compliance – e.g., entity identification to specific transactions
  - Governance of security policies – change control, delegation and consistency

Architectural principles

- Consistent policy enforcement (Runtime)
  - Security as a service - Service orientation
  - Federation through mediation
  - (note: enforcement in this context is inclusive of decision points)
- Externalization of policies from applications
  - Flexibility to deal with change
  - Does not mean applications need to be re-written, necessarily
- Consistent policy management (Administration)
  - Policy Federation
- Experience
  - Model driven security
- Interoperability and integration
  - Open standards

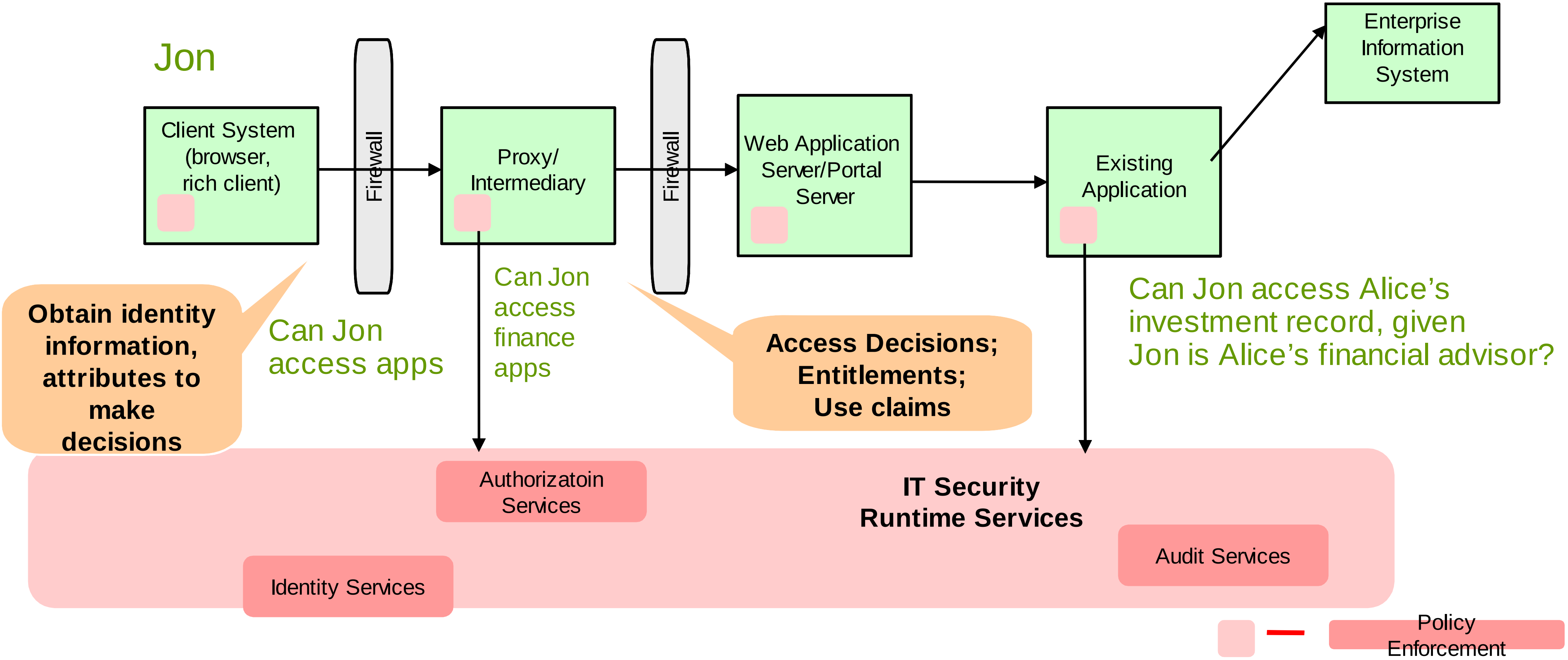
Message Security Policy for Authentication & Identity Propagation

- Applications need end user's identity for controlling access and compliance
- Identity information needs to be mediated for access
- Authentication service
  - How to secure messages for integrity & confidentiality?
  - How to authenticate, validate and transform identity claims/tokens across boundaries


Jon
Client System (browser, rich client)
Firewall
Proxy/ Intermediary
Firewall
Web Application Server/Portal Server
Existing Application
z42
Enterprise Information System
<Jdoe_token>
jdoe@us.ibm.com
jdoe@us.ibm.com
Mapped to z42
Message confidentiality & integrity policies - What to sign? Encrypt?
What identity token? Trust policy?
Authentication Services
IT Security Runtime Services
Identity Services
Audit Services
Policy Enforcement

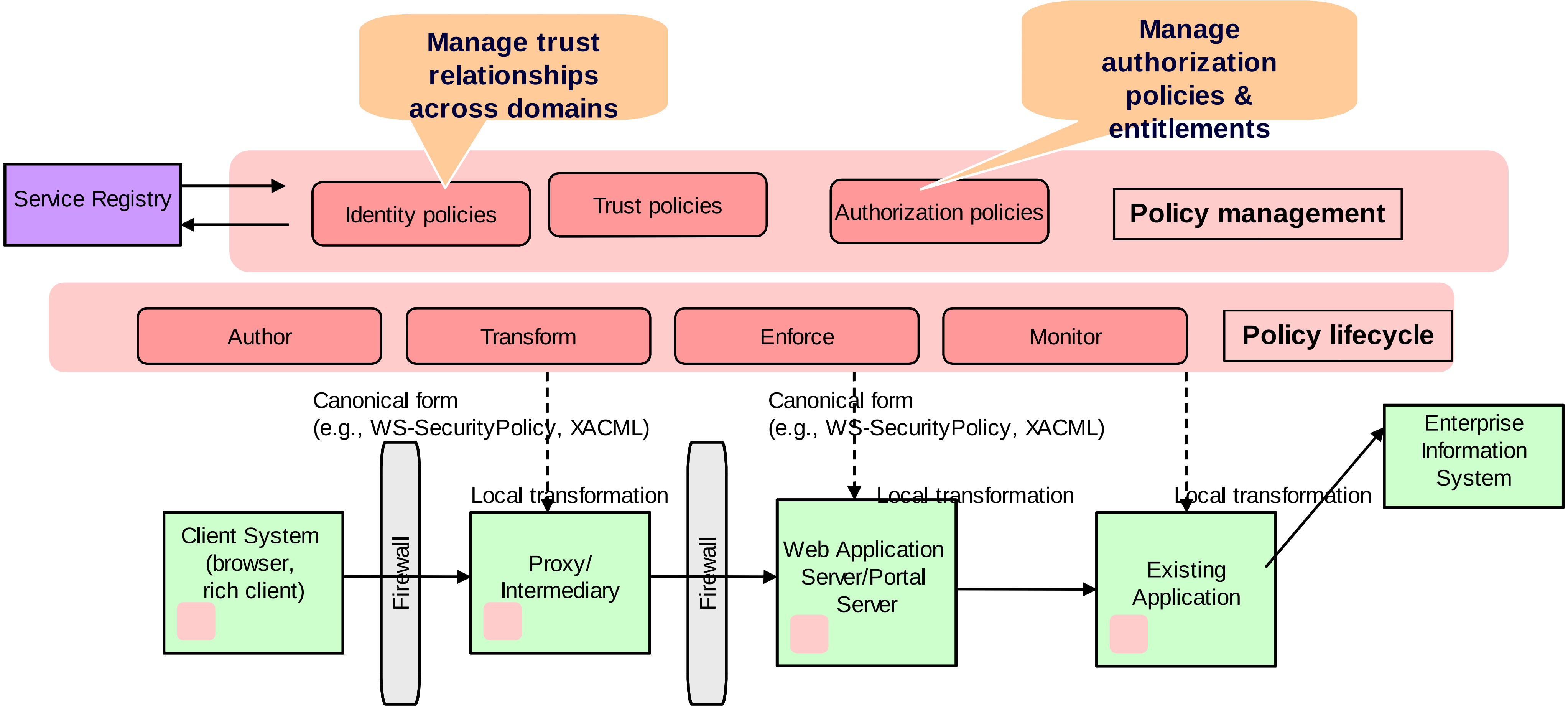
Authorization Policy for Access & Entitlements

- Access decisions to take following into considerations
  - Identity context. resource context, Request context
- Need an efficient way to externalize access control out of application logic
- Authorization service
  - Centralized decision point for access and entitlements

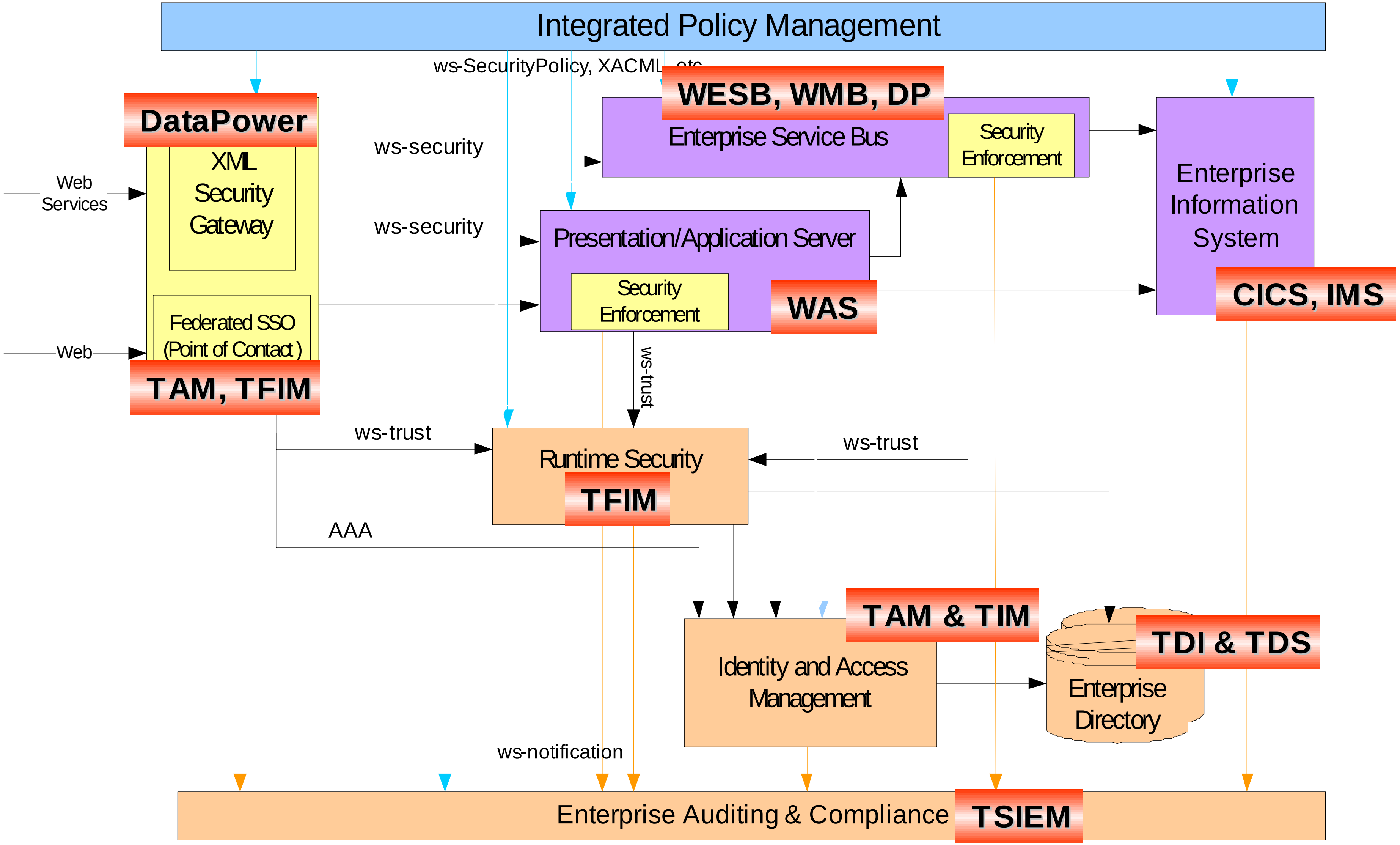

Jon
Client System (browser, rich client)
Firewall
Proxy/ Intermediary
Firewall
Web Application Server/Portal Server
Existing Application
Enterprise Information System
Obtain identity information, attributes to make decisions
Can Jon access apps
Can Jon access finance apps
Access Decisions; Entitlements; Use claims
Can Jon access Alice's investment record, given Jon is Alice's financial advisor?
Authorizatoin Services
IT Security Runtime Services
Audit Services
Identity Services
Policy Enforcement

Security Policy Management

- Multiple heterogeneous enforcement points
- Potential inconsistency in managing policies and configuration across those
- Unified security policy management
  - Federate policies to enforcement points (including decision points/services)
  - Canonical form of policy expressions – and local transformations as necessary


Manage trust relationships across domains
Manage authorization policies & entitlements
Service Registry
Identity policies
Trust policies
Authorization policies
Policy management
Author
Transform
Enforce
Monitor
Policy lifecycle
Canonical form (e.g., WS-SecurityPolicy, XACML)
Canonical form (e.g., WS-SecurityPolicy, XACML)
Local transformation
Local transformation
Local transformation
Client System (browser, rich client)
Firewall
Proxy/ Intermediary
Firewall
Web Application Server/Portal Server
Existing Application
Enterprise Information System

Example Logical SOA Security Architecture


Integrated Policy Management
ws-SecurityPolicy, XACML, etc.
DataPower
XML Security Gateway
Web Services
Federated SSO (Point of Contact)
Web
TAM, TFIM
ws-security
ws-security
WESB, WMB, DP
Enterprise Service Bus
Security Enforcement
Presentation/Application Server
Security Enforcement
WAS
Enterprise Information System
CICS, IMS
ws-trust
ws-trust
ws-trust
Runtime Security
TFIM
AAA
TAM & TIM
Identity and Access Management
TDI & TDS
Enterprise Directory
ws-notification
Enterprise Auditing & Compliance
TSIEM