Business and Technical Insights into Identity, Access and Federation Solutions

Tivoli software

Martin Borrett

Lead Security Architect

Technical Staff Member

NE Europe

IBM SWG

Agenda

- Business background
- IBM Security Solutions for Identity, Access and Federation
  - TIM (Tivoli Identity Manager)
    - Business case
    - Technical capabilities
    - Customer use case
  - TAM (Tivoli Access Manager)
    - Business case
    - Technical capabilities
    - Customer use case
  - TFIM (Tivoli Federated Identity Manager)
    - Business case
    - Technical capabilities
    - Customer use case

Business Challenges - Sound familiar?

Acquisitions and mergers

Inadequate return on investment in IT

Need to streamline linkages with partners and suppliers

External system threats

Increasingly mobile workforce

Legacy system integration

New standards and regulations

Need for a consolidated view of information and applications

More demands for personalized service

Protect security and privacy of critical assets

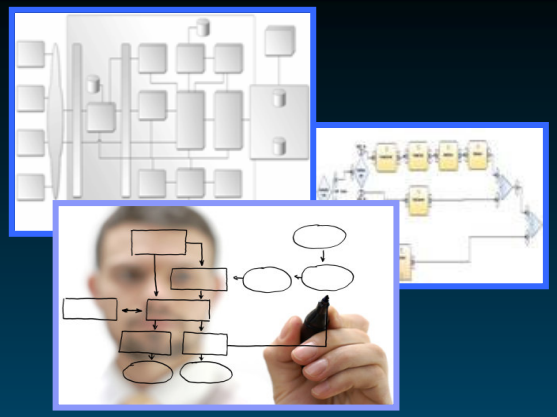
Improve operational efficiency – manage costs

Seamless access to infrastructure anytime/anyplace

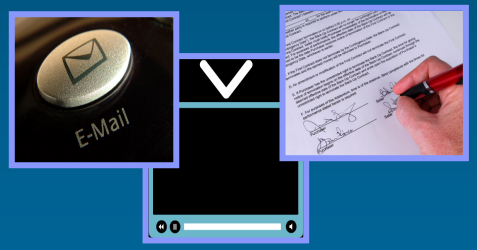
Increasing volume of data

Where are the Risks?

People



Process



Information

Technology

Three Cases for Improving Security

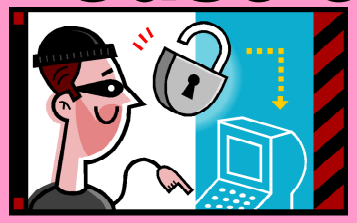
Case 1—The Carrot

ROI

Case 2—The Stick

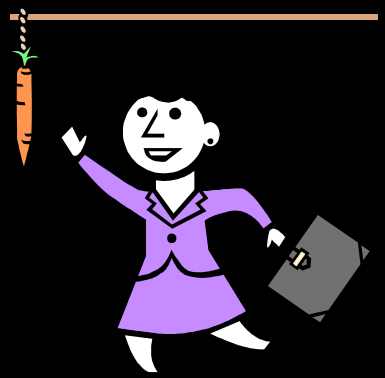
Regs

Case 3—The Fear



Hack

Making the Case with ROI

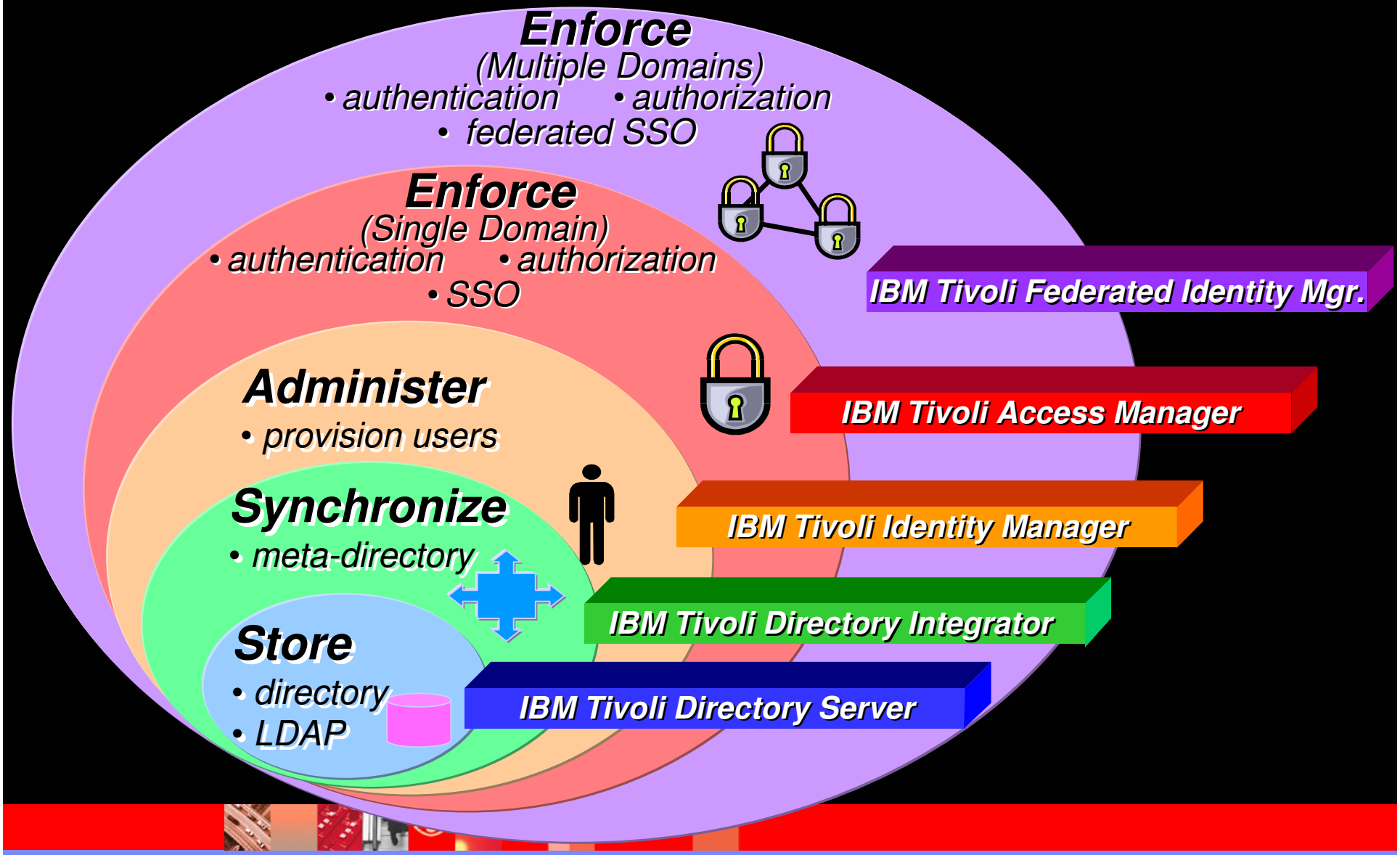


Typical Identity Management Inefficiencies

Provisioning New Users	Elapsed turn-on time for users is up to 12 days
Managing Users	Help Desk costs $20 per call for pw resets
De-provisioning Users	30-60% of existing accounts are invalid
Deploying New Initiatives	Up to 30% of application development time Is for access control

Need to automate complex, administrator intensive Identity Management business processes

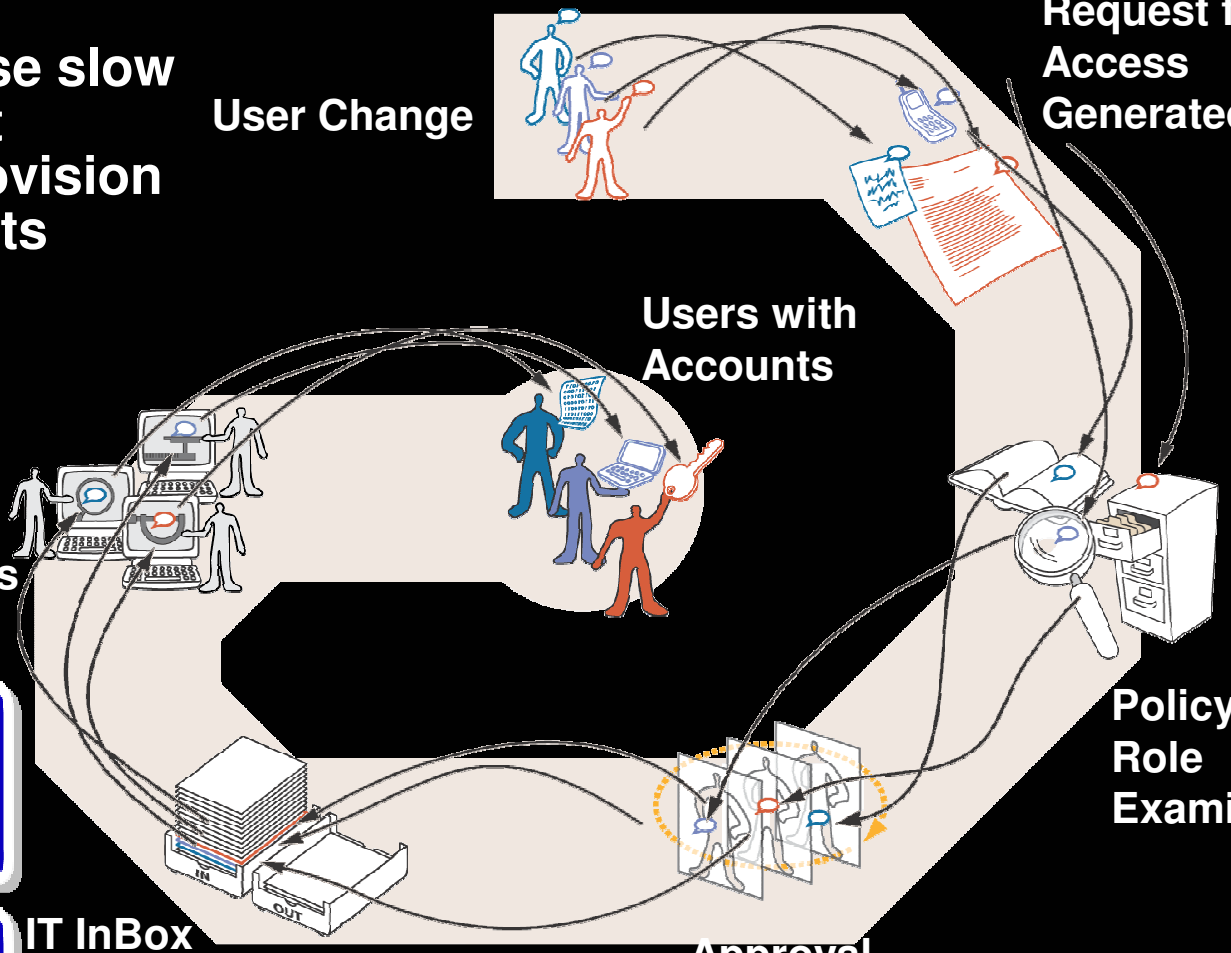
Identity, Access and Federation Management Solutions



Tivoli Identity Manager (TIM)

Manual Provisioning

Organizations use slow and inconsistent processes to provision user access rights



Elapsed turn-on time: up to 12 days per user

Account turn-off performance: 30-60% of accounts are invalid

1 FTE user admin only handles 300-500 users

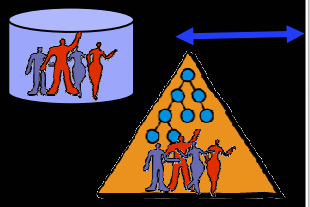
Increase speed and efficiency of security management processes with Tivoli Identity Manager

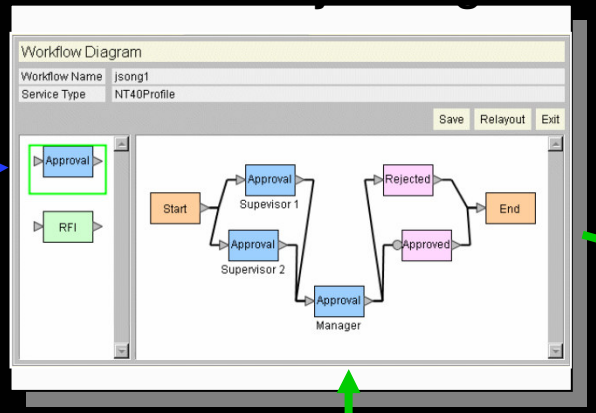
- **Manage changes in minutes, not days**
- **Reduce errors**
- **Free valuable administrators for more productive work**
- **Support scalable business processes**

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





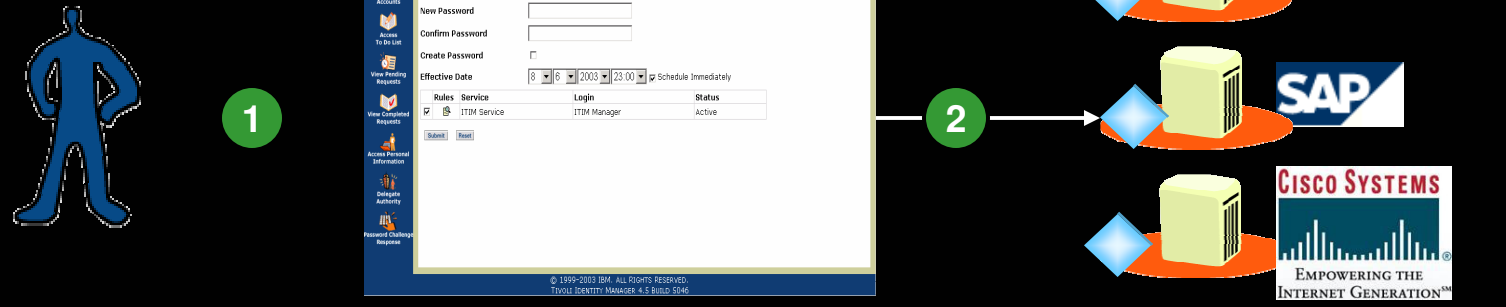
Lower help desk costs and improve user experience via Tivoli Identity Manager self-care

Lower Cost

- Users may service all of their own attributes (address, title, etc)
  - Challenge response for password reset
  - Changes can be reviewed/approved via workflow
- User self-service password resets across all systems
- Challenge-Response system for forgotten passwords
- Synchronize passwords and IDs across all systems
- Password Rule Checking

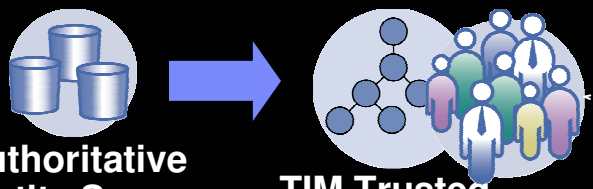
Help Desk costs $20-per-call for password resets
Gartner Group

Employees request an average of 3-4 reset per year
Meta Group



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

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



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

TIM Trusted Identity Store

John C. Doe

Sarah K. Smith

jcd0895

jdoe03

Sarah_s4

nbody

Business Applications

1

Eliminate orphan accounts

ackerh05

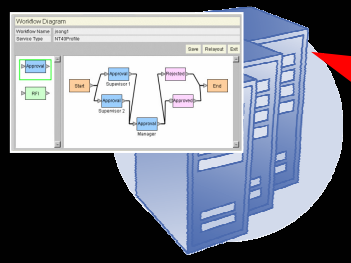
Cisco Secure ACS

doej

smiths17

2

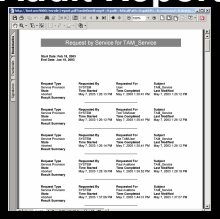
Compare local privileges to policy



Identity Manager Policies and Approvals

3

Audit Reports

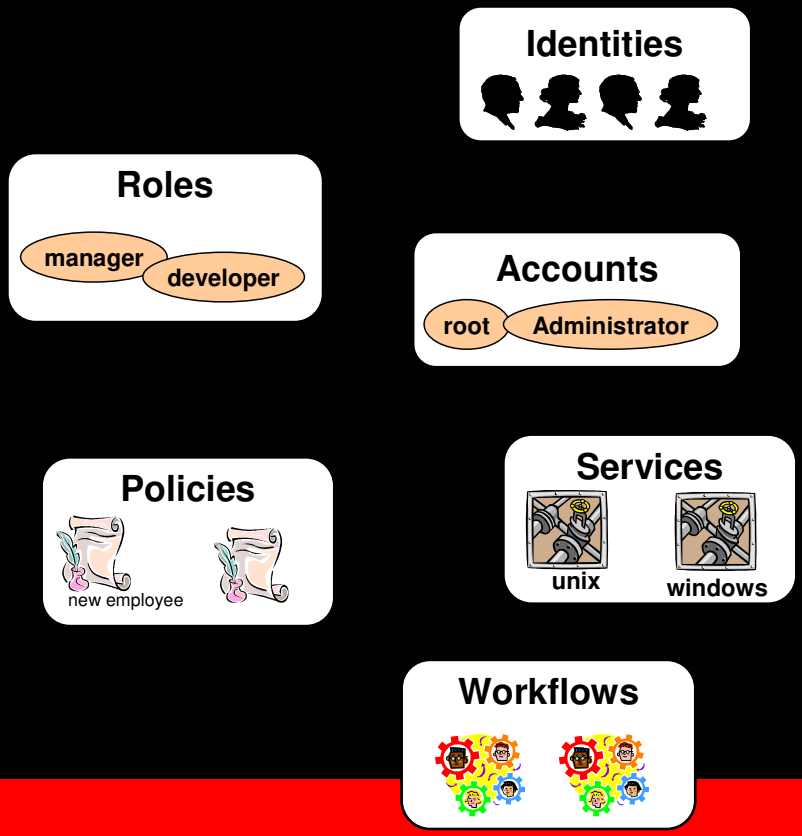


Flag/Correct/Suspend

Automated, Role Based Access Provisioning

Fully automate granting and revoking of access rights

- **Access rights automatically granted as job responsibilities change**
- **Locks down potential access to appropriate groups of people**
- **Increases business scalability and eliminates administrative effort**
- **Automatically removes access upon job change or separation**



Industry leading agentless adapters accelerate time to value

Authentication & Security

IBM RACF zOS*
IBM Tivoli Access Manager
CA ACF2
CA Top Secret
Entrust PKI*
RSA ACE/Server*
CA Siteminder
Oracle Netpoint
Cisco ACS*

Relational Database

IBM DB2/UDB
Informix Dynamic Server
Oracle
Microsoft SQL Server 2000
Sybase
RDBMS-based Applications

Applications & Messaging

Amdocs ClarifyCRM *
EMC Documentum *
Lotus Notes/Domino
Windows Exchange 2000, 2003
Novell e-Directory (NDS)
Novell GroupWise
Oracle E-Business Suite
PeopleSoft (People Tools)
SAP Enterprise Portal 6
SAP R/3
Siebel
Peregrine Service Center
Remedy
IBM Rational ClearCase
LDAP-based Applications
Command Line-based Applications*
Universal Provisioning – for Manual Applications

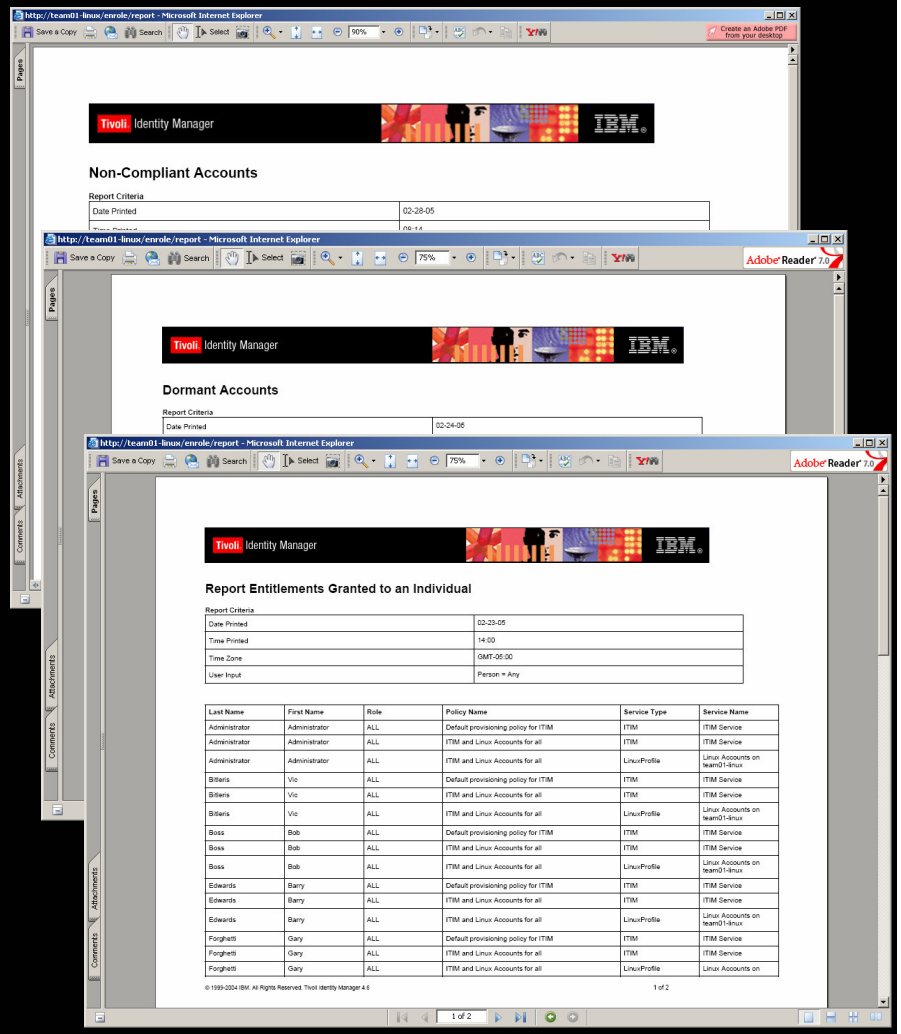
Operating Systems

HP/Compaq Tru64 Unix
HP-UX
HP-UX NIS
IBM AIX
IBM AS/400*
OpenVMS*
RedHat Enterprise Linux
Sun Solaris
Sun Solaris NIS
SuSE Linux Enterprise Server
Windows Active Directory
Windows Local 2000, 2003, XP

Design Characteristics:
- **Secure**
- **Bi-directional**
- **Firewall friendly**
- **Network friendly**

Quickly produce comprehensive audit reports

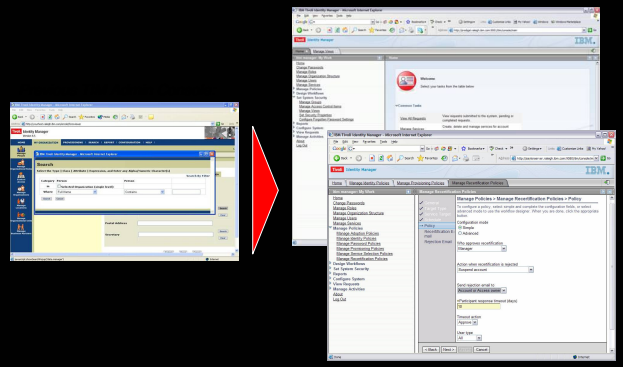
- Default and custom reports
- Centralized view of people and privileges
- Track access privileges by person
- Track access privileges by information resource
- Acrobat format for easy viewing and CSV format for custom analysis
- Crystal Reports integration and support



Major updates in TIM 5.0 deliver innovations in usability, time to value, and identity governance

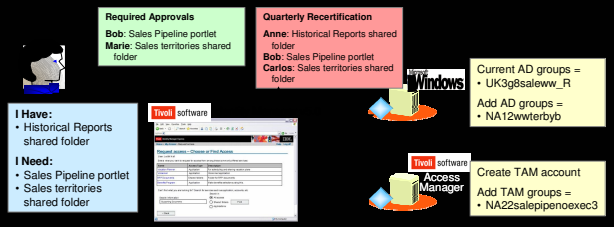
At a Glance

- World Wide Release: December 12, 2007
- 40+ Beta participants
- Up to 50% faster rollout



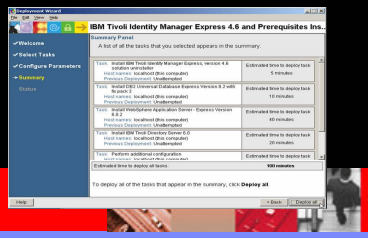
Intuitive User Experience Adaptable to Corporate Branding Needs

- "Make the simple things simple"
- **Business-friendly provisioning requests and approvals via group management**
- **Request and approve role membership**
- Tailored, configurable user interface views for different user types
- Look and feel customizable via style sheets and custom text – "skinnable UI"
- Task oriented wizards and smart searches
- Section 508 Accessibility compliance



Automated Compliance Lifecycle

- **Business-friendly revalidation of granular user access rights**
- Auditor-centric UI view and reports
- Additional compliance related reports
- Includes new Tivoli Common Reporting module and TCIM integration



Simplified Deployment Options

- **Upgrade from TIM Express to TIM**
- **Single server launch pad installer**, simplified middleware and fixpack application

ING Group

Industry: *Banking*
Profile: *One of the 20 largest financial institutions in the world with more than 60 million clients in over 50 countries*
Size: *10,000 or more*
Category: *IT Strategy and Architecture Services*

Client requirements

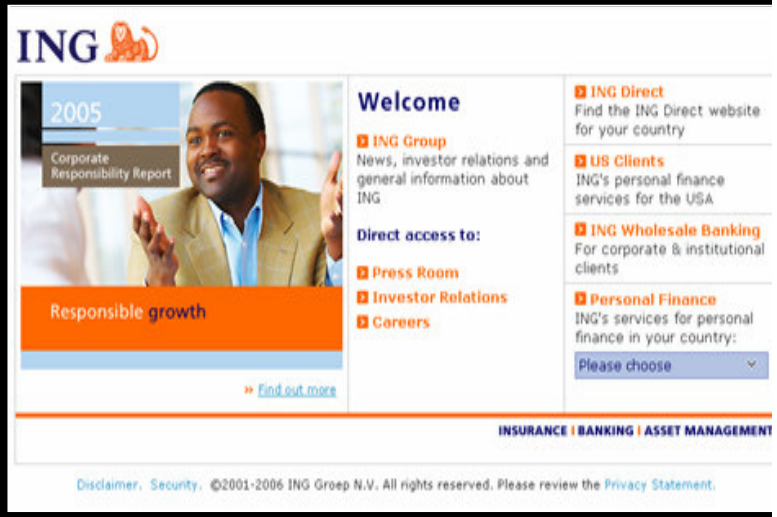
- Improve its ability to manage and secure access rights for 113,000 internal employees by replacing manual- and paper-based methods with automated processes
- Shorten the time needed to comply with government regulations

Solution

- Worked with IBM Global Technology Services to deploy an automated access-rights management solution based on IBM Tivoli® Identity Manager, IBM Tivoli Access Manager and IBM Tivoli Directory Integrator software
- Optimized server support for the security solution using IBM eServer™ pSeries® 650 servers

Benefits

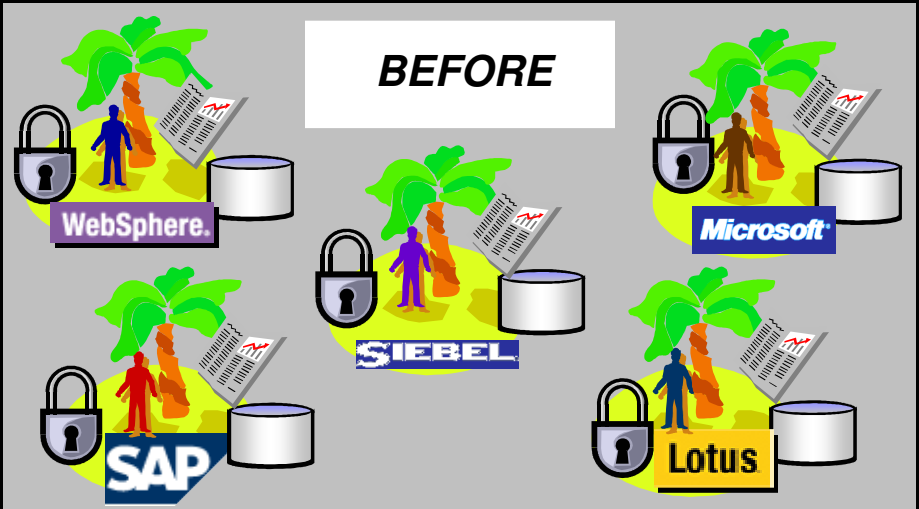
- Reduced the time required to assign access rights to new users from 10 days to less than 24 hours
- Will enable a savings of €15 million per year through automation
- Reduced help-desk costs by 25 percent through self-service features



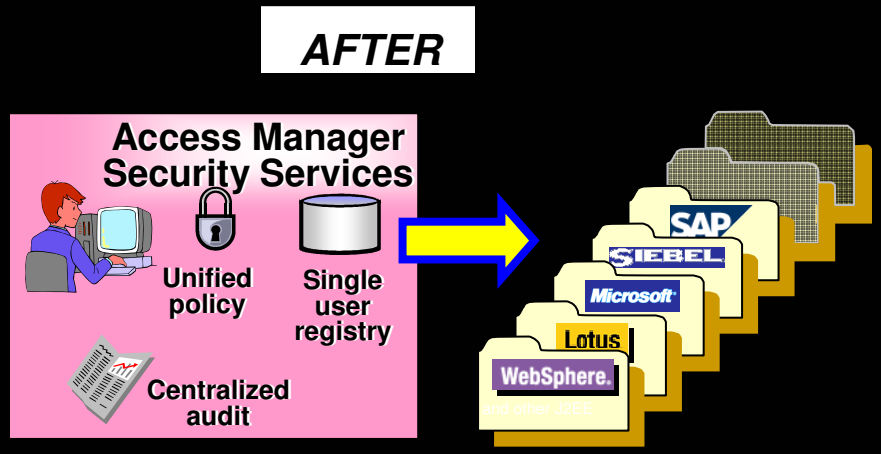
ing.com

Tivoli Access Manager (TAM)

Tivoli Access Manager for e-business (TAM)



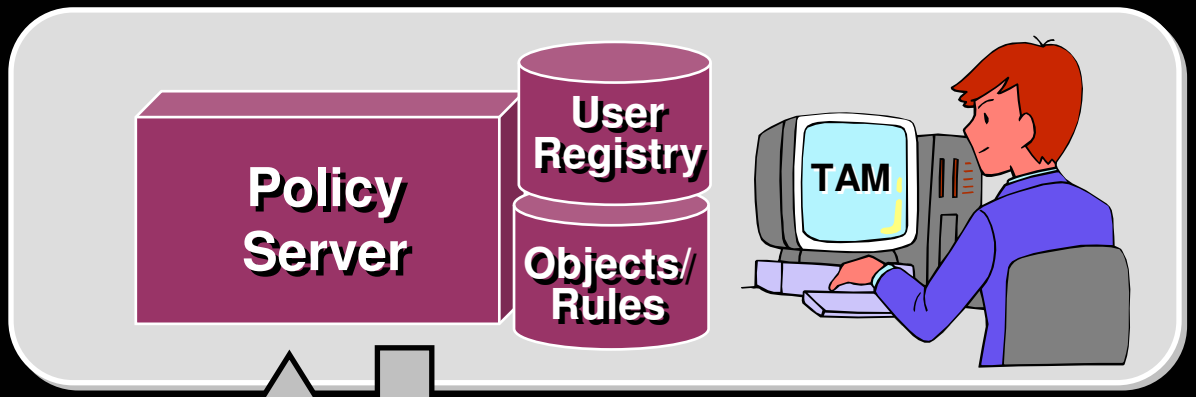
- Too many passwords to remember
- Multiple admins with multiple access control tools
- User and access control information everywhere
- Compliance? To what?



- Web single sign-on
- Single admin or delegated admins with a single tool
- User and security info centralized/ understandable
- Policy + audit = compliance

= Security policy = User & group info = Audit

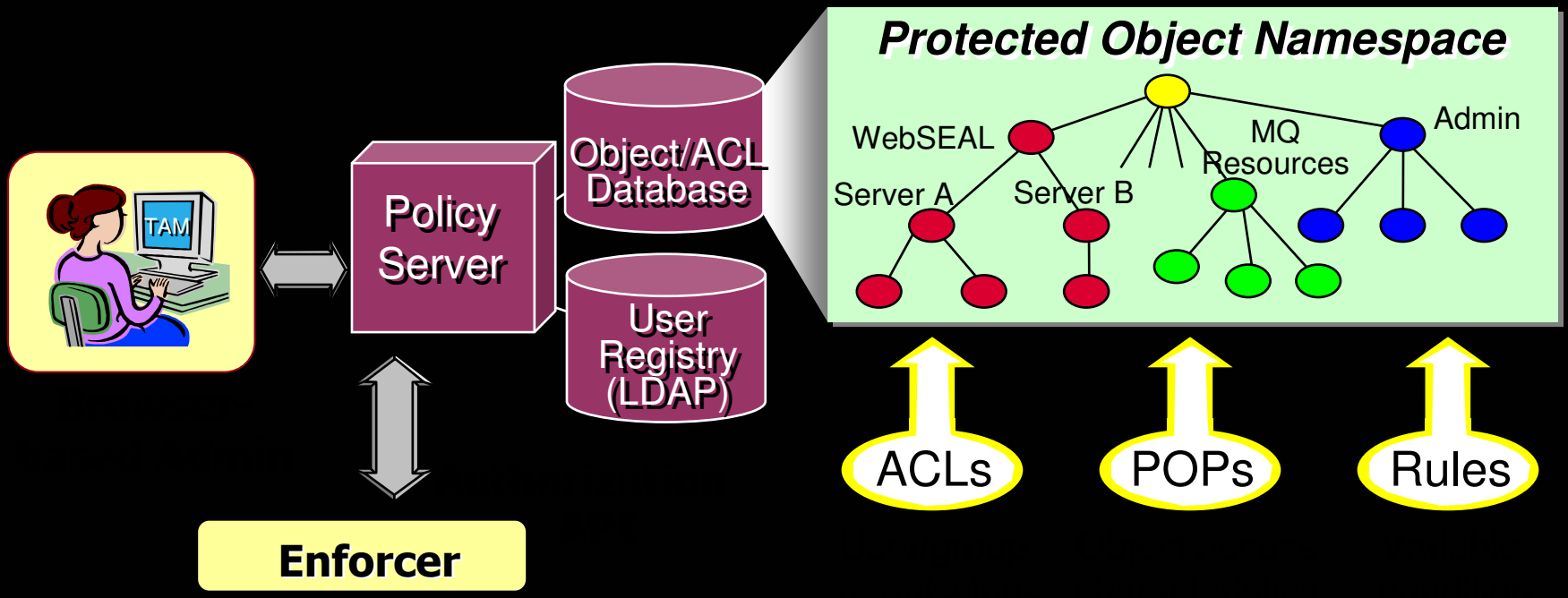
A Robust Model for Authorization



Input:
- Identity
- Object
- Actions

Result:
- Yes
- No

Establishing Clear Rules for Access Decisions



- **Web-based Management Console** (Delegatable admin)
- **Policy Server** (Master Authentication/Authorization Services)
- **Unified Security Policy** (Policy Templates applied to Namespace)
- **Single, Consistent Authorization Approach**

Access Manager Family—Breadth of Coverage

Single Protected Object Namespace!

Web/URL
- URLs
- CGI Programs
- HTML files
- Java servlets
- Java class files

AMeb

UNIX/Linux Systems
- Fine-grained authorization for system/network actions

AMOS

AMeb

AMBI

WMQ, WBI Brokers
- End-to End Data Protection
- Central Security Admin

AMeb

AMeb

AMeb

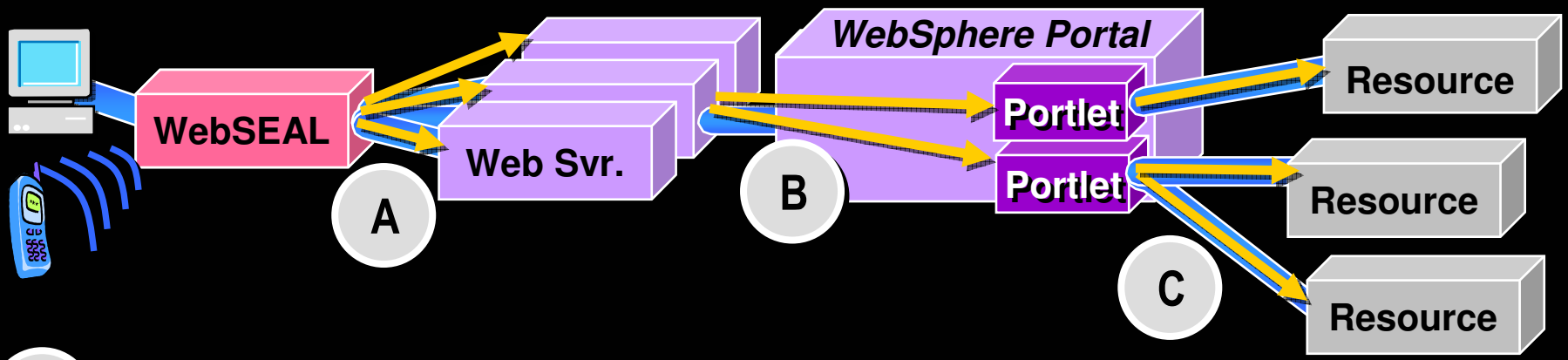
Web Application Servers
- IBM WebSphere
  - Application Server
  - Edge Server
  - WAS Network Deployment
  - WebSphere Everyplace Suite
- BEA WebLogic
- *Any* other via J2EE, JAAS, and/or aznAPI

Mainframe
- Secure 3-tier Web transactions
- CICS, IMS, DB2, TSO, …
- Leverages JCA/WebSphere/TAM
- Integrated with RACF

Lotus Domino
- Domino
- iNotes
- QuickPlace
- Sametime

Key Portal / Web Solutions
- WebSphere Portal
- PeopleSoft PeopleTools
- Siebel 2000
- SAP Enterprise Portal
- and more . . .

Layers of Authorization



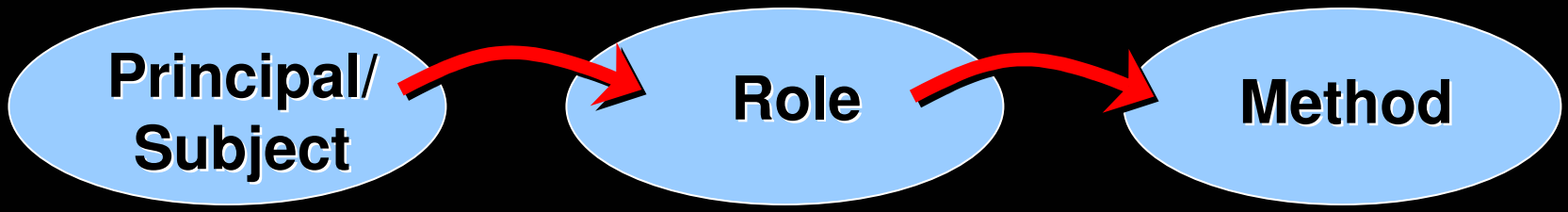
A Web URL Layer. TAMeb controls access.

B Portlet Layer. Customer choice (TAMeb or WPS control).

C Business Logic Layer. TAMeb's Java and .NET support

J2EE Security Overview & TAM for WAS

- ***Two mappings are very important to J2EE security:***



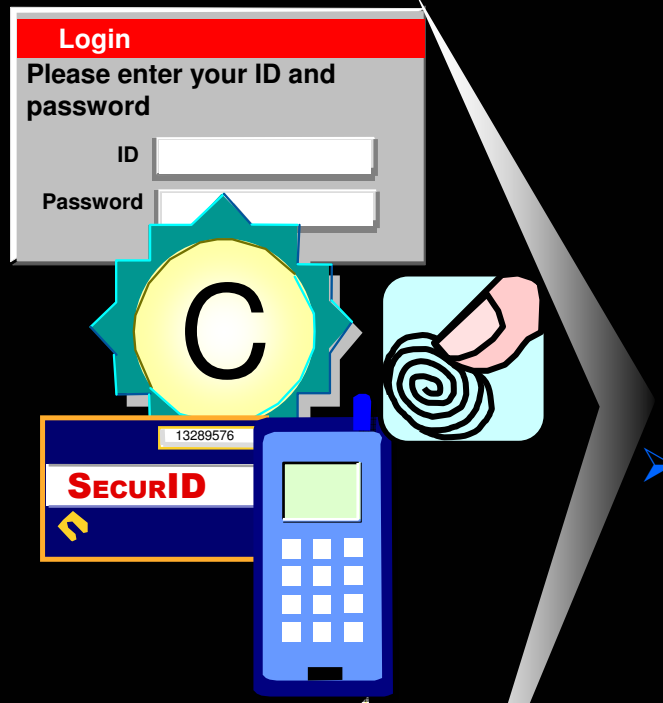
- Principal/subject to Role
- Determined by Administrator
- Relatively dynamic

- Role to Method
- Determined by Deployment Descriptor

ACCESS MANAGER FOR E-BUSINESS

- Can handle Principal/Subject-to-Role mapping for WAS
- Can handle Role-to-Method mapping (via TAMeb JACC provider)

How Do I Authenticate Users?



Easy accommodation of authentication methods and other security

support here

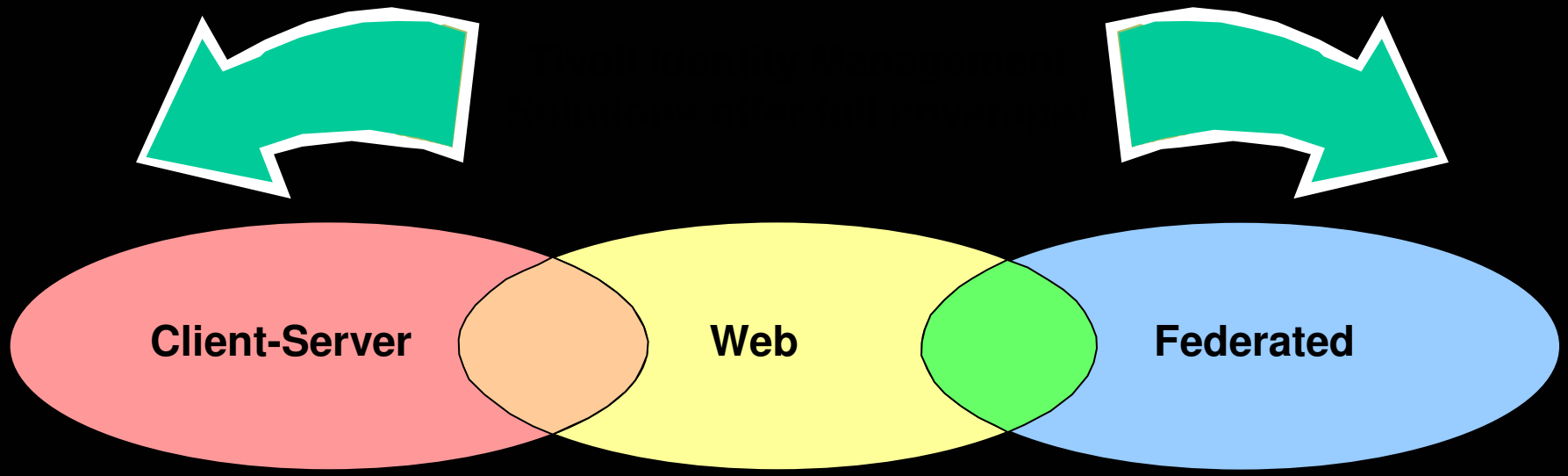
Access Manager

reap value here

WebSphere.
PeopleSoft
SIEBEL
Microsoft
Lotus
VIGNETTE
SAP
& more

- **Prove incoming users identity**
  - Basic authentication
  - Forms-based authentication
  - X.509 Certificate
  - Kerberos ticket
  - RSA SecurID Token
  - Mobile device
  - Others via Pluggable Authentication
- **Acquire credentials for user** for use in session management

User Productivity: Single Sign-On

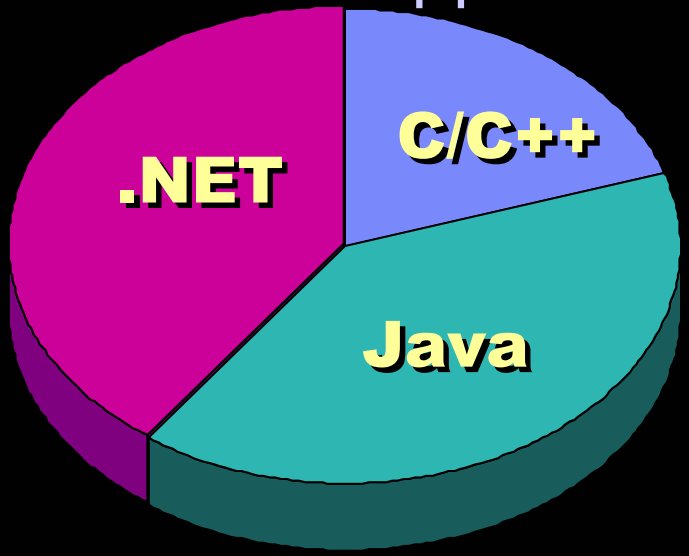


Tivoli Access Manager for e-business

Tivoli Access Mgr. for E-SSO

Tivoli Federated Identity Manager

TAM supports ASP .NET Applications



- **SOA approach for authentication/authorization now applies to .NET as well as C/C++ and Java**
- **Includes:**
  - SSO from WebSEAL or Web Svr. Plug-In to ASP.NET application
  - Role membership evaluation using TAM policy (declarative programming approach)
  - Exposure of TAM APIs to .NET applications (programmatic programming approach)
  - Web service security

Integration Factory

IBM Intranet Integration Factory Home
Newsletters
Integrations
TAMeB
TAMOS
TRM
TPM
TIM
TDI
TFIM
Resources
About Us
Contact Us
IF RSS Feeds
Site Map
Feedback

IF RSS Feed

Add Firefox IF Search (to Firefox Browser only)

Page History:

- Home
- Integrations
- TFIM Integrations

Nov 11, 2007

Integration Factory > Integrations

Integration Factory - Integrations

The following tables provide a summary of the solutions that are currently available to integrate Tivoli security products with IBM and non-IBM products.

Select the appropriate row and column for the vendor product and Tivoli security product you are interested in. If the table indicates that an integration solution exists, click the link to view details of the latest integration solution for the newest version of the ISV product.

Note that integration solutions may not cover all OS platforms, Tivoli security product versions or integration product versions. Check the details carefully to ensure that the solution meets your integration needs.

To access integration solutions for older product versions, click the Tivoli security product link in the column title. This link provides all available integration solutions for the particular Tivoli product, as well as additional Tivoli product information.

To view all integration solutions for a particular vendor product, click on the row title (this feature is not currently available for all vendors).

IBM Products | **ISV Products** | Technology & Standards | Tivoli Ready | Other

Integration Solutions with ISV products

Vendor	Product	TAMeB	TAMOS	TRM	TPM	TIM	TDI	TFIM
Aelita	Directory Manager 4.1	YES						
Amdocs	Clarify CRM					YES		
BEA	Weblogic 9.0, 9.1, 9.2, 10.0	YES						YES
BMC	BMC Remedy					YES		
BroadVision	One-to-One Enterprise 6.0, 7.0	YES						
	Presentation Server 3.0	YES						
CheckPoint	Firewall-1 NG			YES				
	Firewall NG AI R55			YES				
Cisco	Cisco ACS					YES		
	Secure PIX Firewall 5.1-6.3			YES				
	Secure PIX Firewall 5.2			YES				
	Secure PIX Firewall 6.3-7.0			YES				

Access Manager ecosystem – Direct plus 'Ready for Tivoli'

Application Single Sign-On
- Adexa collaboration products (9)
- Blockade ESconnect
- Broadvision One to One
- Cash-U Pecan
- Centric Product Innovation (3)
- Citrix Metaframe
- Citrix NFuse
- IBM Content Manager
- IBM Host on Demand
- IBM Host Publisher
- Intelliden R-Series
- Kana Platform
- Kintana (Mercury Interactive)
- Lotus Domino
- Lotus iNotes
- Lotus Kstation
- Lotus Quickplace
- Lotus Sametime
- Lotus Team Workplace
- Microsoft Exchange (OWA)
- OpenConnect WebConnect
- Oracle Enterprise server
- PeopleSoft PeopleTools
- Rocksteady NSA
- SAP Enterprise Portal
- SAP ITS
- Secur-IT C-Man
- Secur-IT D-Man
- Siebel
- Sourcefire ISM
- Sun Calend
- Sun Messenger Server*
- Vasco Digipass (via C-Man)

Desktop SSO
- ActivCard ActivClient
- Microsoft Kerberos (SPNEGO)
- Microsoft NTLM

Directory sync & virtualization
- Aelita Ent. Directory Manager
- IBM Tivoli Directory Integrator
- OctetString Virtual Directory
- Radiant Logic

Encryption, SSL & VPN
- Aventail EX-1500
- Eracom ProtectServer Orange
- IBM 4758
- IBM 4960
- nCipher nForce
- Rainbow Technologies Cryptoswift

Integration and Consulting
- Accenture
- Deloitte & Touche
- EDS
- IBM Global Services

Plus many other local SIs such as ePresence, Secur-IT, ECSSC and Sena Systems

Messaging security
- IBM WebSphere BI Message Broker
- IBM WebSphere BI Event Broker

Platform & Traffic Mgmt.
- Crossbeam Security Svcs. Switch
- F5 Networks BIG IP
- Sanctum AppShield

Reporting and Audit
- Business Objects Crystal Reports
- Tivoli Enterprise Console
- Tivoli Risk Manager

Audit capabilities in XML and comma-delimited for wide integration

Strong Authentication
- ActivCard
- Aladdin Knowledge Systems
- Daon Engine (Biometrics)
- VeriSign

UNIX Deployment Lockdown
- HP-UX
- IBM AIX
- IBM DB2
- IBM HTTP Server
- IBM WebSphere App. Server
- Oracle DB
- Red Hat Linux
- Sun Solaris
- SuSE Linux

User repository
- CA eTrust Directory
- IBM Tivoli Directory Server
- Microsoft Active Directory
- Novell eDirectory
- Siemens Nixdorf DirX Directory
- Sun ONE Directory Server

Web Server Plug-in
- Apache
- IBM HTTP Server
- IBM WebSphere Edge Server
- Microsoft IIS
- Sun ONE Web Server

Web Application Server
- BEA WebLogic Server
- IBM WebSphere App. Server (Any J2EE Platform)
- Microsoft .NET

Web Portal Server
- BEA WebLogic Portal (SSO)
- IBM WebSphere Portal
- Plumtree Portal*
- Sun ONE Portal Server (SSO)

XML and Web Services
- Datapower
- Digital Evolution Service Manager
- Layer 7 SecureSpan Gateway
- Reactivity XML Firewall
- SAML add-on
- VordelSecure

T. Rowe Price

Financial Services

Tivoli Federated Identity Manager, Tivoli Access Manager for e-business, WebSphere Portal Server

Business Challenge

- ✓ Leading financial services firm needed to quickly deploy new SOA- and web-based business services while increasing internal efficiencies

IBM Solution

- ✓ Control: Securely connecting 2.5 Million identities across new business services and within corporate intranet with IBM Tivoli Access Manager for e-business and WebSphere Portal Server
- ✓ Automation: Automated application of proper access control policies across 400+ business services

Business Value

- ✓ Deployed new web services-based business services to clients in a fraction of the time it would have taken to develop the services themselves
- ✓ Immediate integration across corporate intranet and customer-facing portal for employee retirement planning
- ✓ Saved $24M in application development costs over 8 years by centralizing application security controls
- ✓ Reduced help desk password reset calls by 61% with web-based single sign-on support

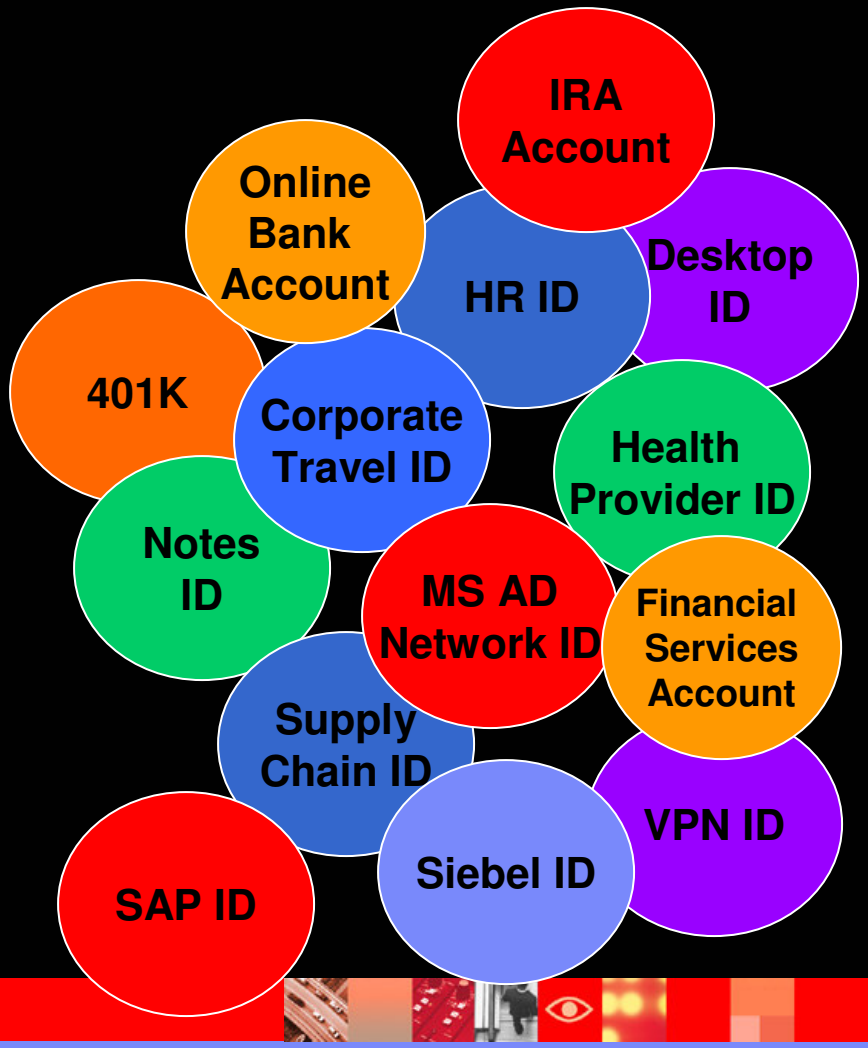
Securely integrate new corporate clients with online retirement plan information in Days

Reduced help desk costs for password reset calls by 61%

Covers 2.5 million users across 400 applications

Tivoli Federated Identity Manager (TFIM)

Multiple Identity Problem



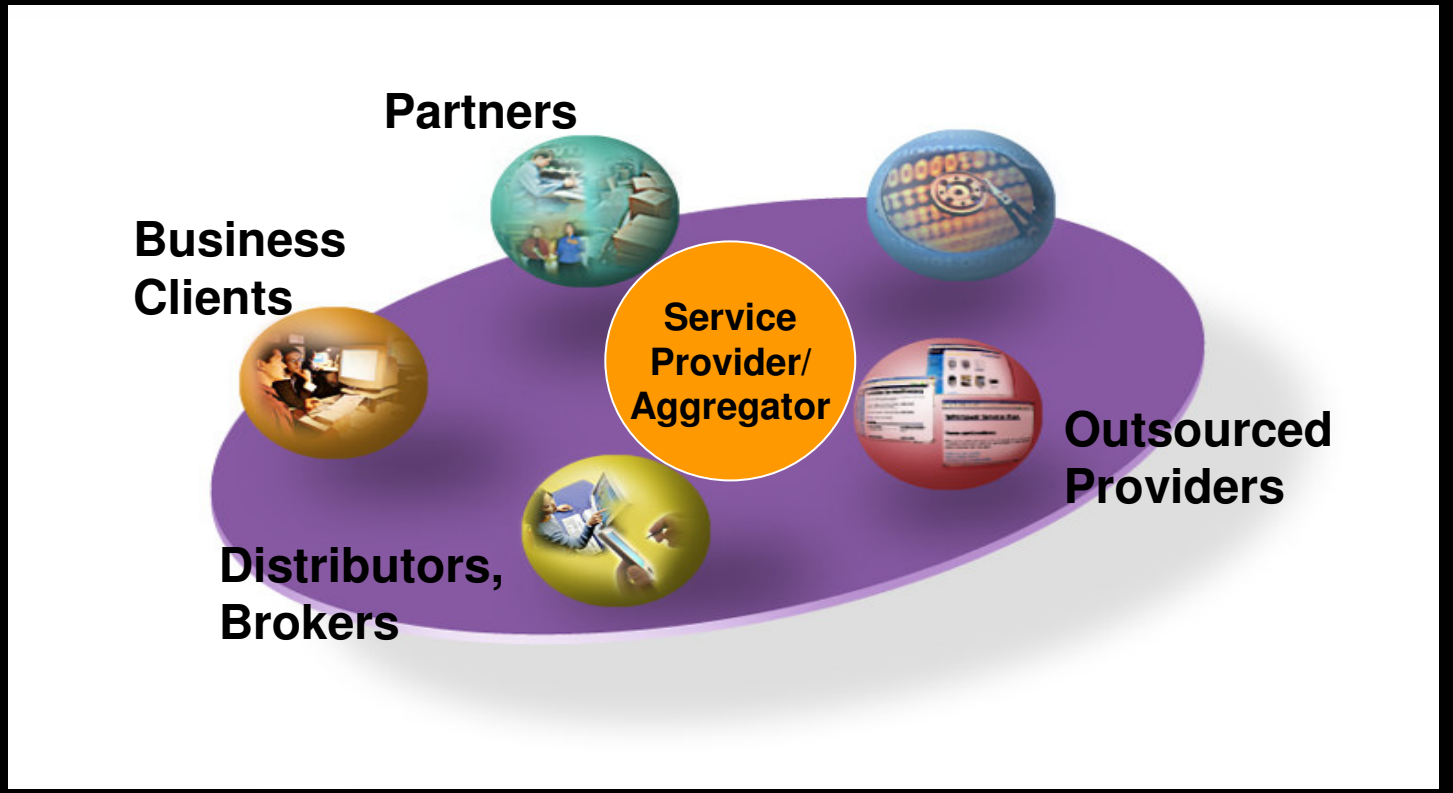
Each application brings its own ID

Each ID does not work with other IDs

Each ID adds cost and complexity

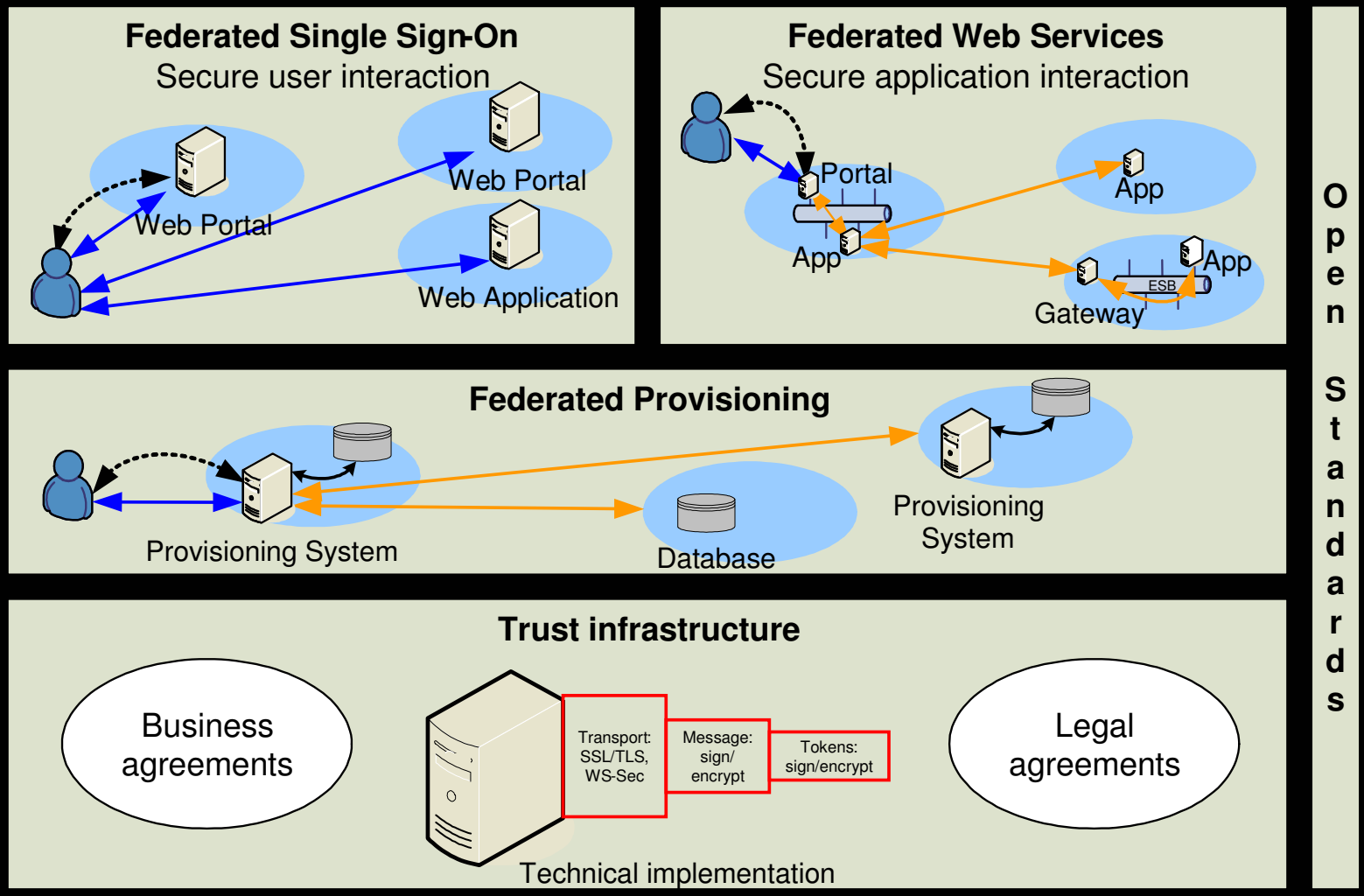
Each ID adds business risk to compliance with business, regulatory, legal and security requirements

Problem: Ineffective Identity Management

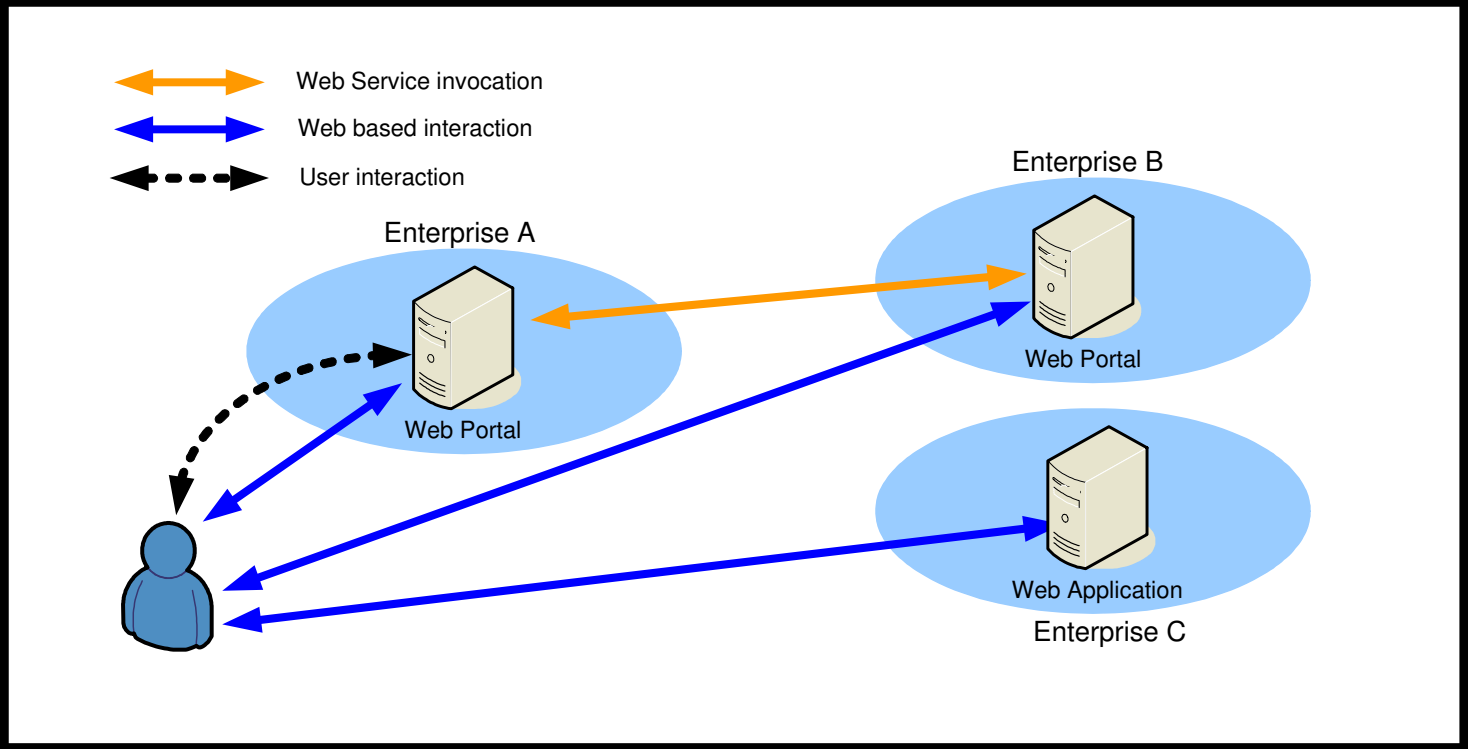


1. Today, companies have no way to "trust" identities belonging to their partners, suppliers, contracts and their outsourcers.
2. Lack of trust means companies end-up creating online identities (and passwords) for all users
3. This approach is very costly, inefficient & creates user frustration with multiple accounts and registrations for each Web Site.

Federation Use Cases



Federated Single Sign-On



- **Identity Provider** (IdP)
  - creates, maintains, and manages identity information for users and provides user authentication to other service providers within a circle of trust.
- **Service Provider** (SP)
  - provides services and/or goods to users.

What is Federated Identity?

- Federated Identity Management (FIM)
  - Identity lifecycle management
    - Provisioning of users and linking of user identities
  - Identity mapping across partners
    - Single-sign-on
    - User information exchange
  - Secure application interaction
    - Using web services technology
- Federation requires a trust infrastructure
  - Enables the on-line equivalent of real-world business relationships

Why is this important?

- Lower Identity Management costs
  - Only Identity Providers have to manage authentication information
  - Service Providers manage information relevant to their service
- Enables “Service Oriented Architecture”
  - Services can be offered (securely) to all end users of the federation
    - Good for both Identity Providers and Service Providers
  - Simplify user experience with Single Sign On
- Automation of Provisioning between companies
  - Provisioning of user identities, entitlements and business services
  - Current manual method is costly and time consuming

Benefits of Federation

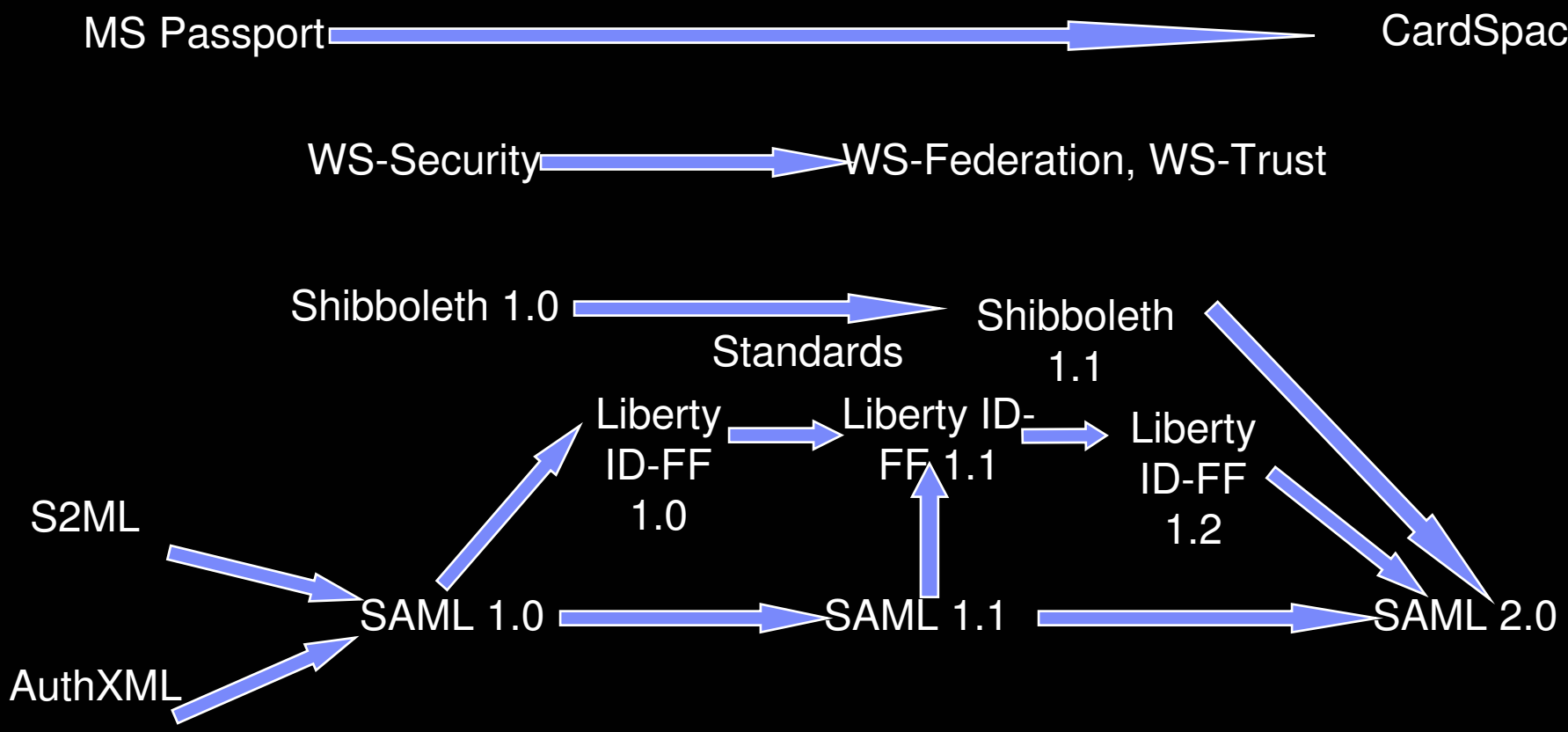
- Users
  - Only one place to update Personal Information
  - Only one authentication required
- Identity Providers
  - Maintain a close relationship with the user
  - Offer 3rd party services seamlessly
- Service Providers
  - Reduced/removed need for local identity management
    - SP can focus on managing only SP relevant information about users
  - Easier access to all users in the federation

“Federation” SSO Efforts

- SAML
- Liberty
- WS-Federation
- CardSpace
- OpenID
- Higgins

(Protocol/Token/Profile)

The Standards Journey …



IBM Tivoli Federated Identity Manager (TFIM)

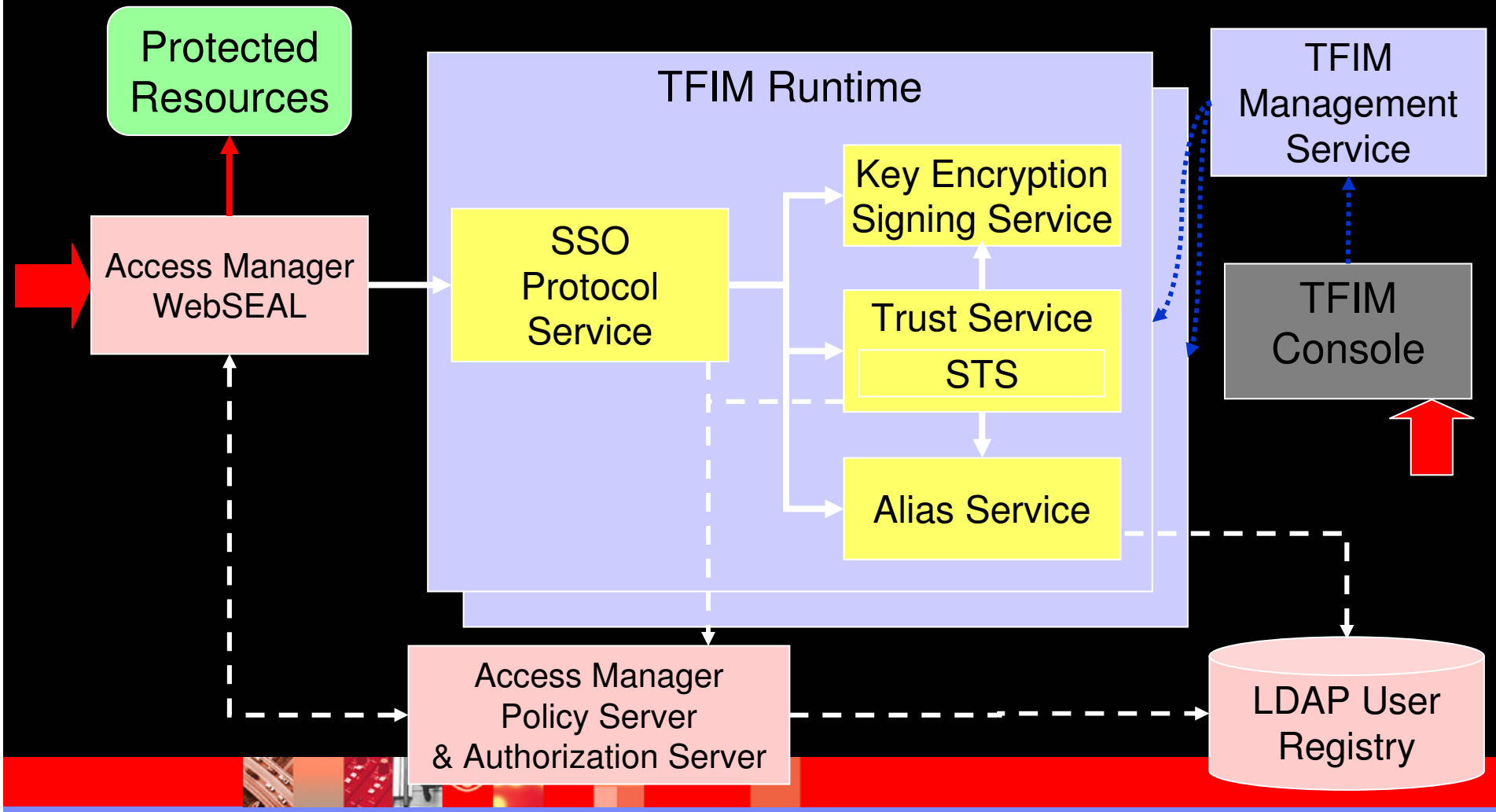
- Single Sign On Services
  - Provides runtime implementation of SSO protocols and profiles
    - Provides COMPLETE session lifecycle, not just SSO
  - May include a specialized Identity/Alias Service
    - Enhanced SSO through management of aliases used within SSO protocols
  - Will in turn leverage a Trust Service
- Trust Services
  - Manages trust infrastructure between partners
  - Will in turn leverage
    - Token Services
    - Identity/Attribute Services
    - Key Management Services
- Web Services Security Management (WSSM)

Federated Single Sign-On

- Integration with IBM Tivoli Access Manager (TAM)
  - Application is shielded from complexity of Federated SSO protocol(s)
    - (Lightweight) SSO to application container, and/or
    - Application can access user identity and attributes from HTTP Headers
  - Concurrent Federated SSO protocol support
    - New versions can be supported without changes to the applications
  - No proprietary APIs
  - Faster time to deploy new application to Federated SSO environment
  - Centralized management of partners' metadata and certificates
    - Provided by TFIM – not part of application development scope (save time/$)

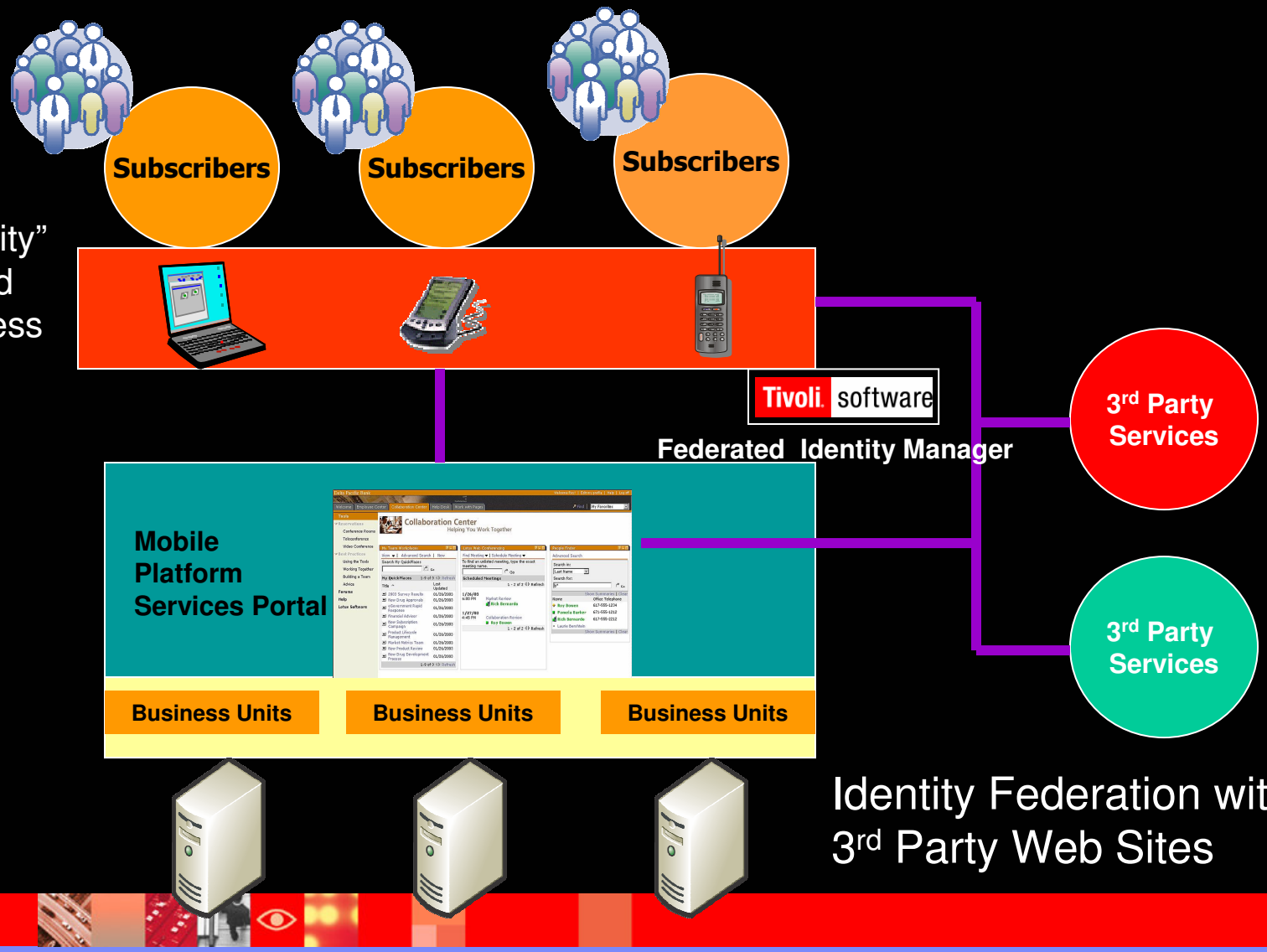
- Supported Protocols:
  - SAML 1.0 / 1.1 / 2.0
  - WS-Federation
  - Liberty ID-FF 1.1 / 1.2

TFIM Components for Federated SSO



Use Cases

Telecommunications - SDP (inc IMS)



Federated SDP: business objectives

- Improve time-to-market for new services offerings
- Offer access to external services without disclosing its customers database
- Deploy a flexible and scalable architecture based on standards
- Reduce total cost of ownership

Services offered per the SDP Platform

- One platform :
  - One portal
  - One technical infrastructure
  - Consistent, high quality, flexible and personalized environment

- A SDP platform can offer the following services :
  - For Consumer / end-user : email, PIM, chat, Kiosk, portals
  - For B2E (Business to Employees) : email, groupware, customer database access…
  - For B2B :
    - communications hub (SMS, MMS),
    - user context, content push
    - device management,
    - service directory.

- Services and applications are available through :
  - Mobile Device (WAP)
  - Internet

Government

- Multiple use cases seen, majority based around connecting citizen portals or identity services to government services whether central or local.

Four Waves of Government (an I/T perspective)

- Online Government
  - Putting services and information online and available 24x7
  - Reduce cost by providing data before demand
- Interactive Government
  - Right location that aggregates all services
  - Citizens access information as well as perform multi-step transactions

Four Waves of Government (an I/T perspective)

- Integrated Government
  - Focus shifts to integrating processes to provide services
  - Centralized security administration outside of web applications
  - Streamlined integrated identity management
  - Business processes aligned with I/T tools, technology infrastructure, I/T service delivery discipline

- End to End e-Government
  - Integration across partners, suppliers, citizens and customers
  - Integration across government and NGOs
  - Government and businesses are interdependent on each other for complimentary services
  - I/T provides a Service Oriented Architecture

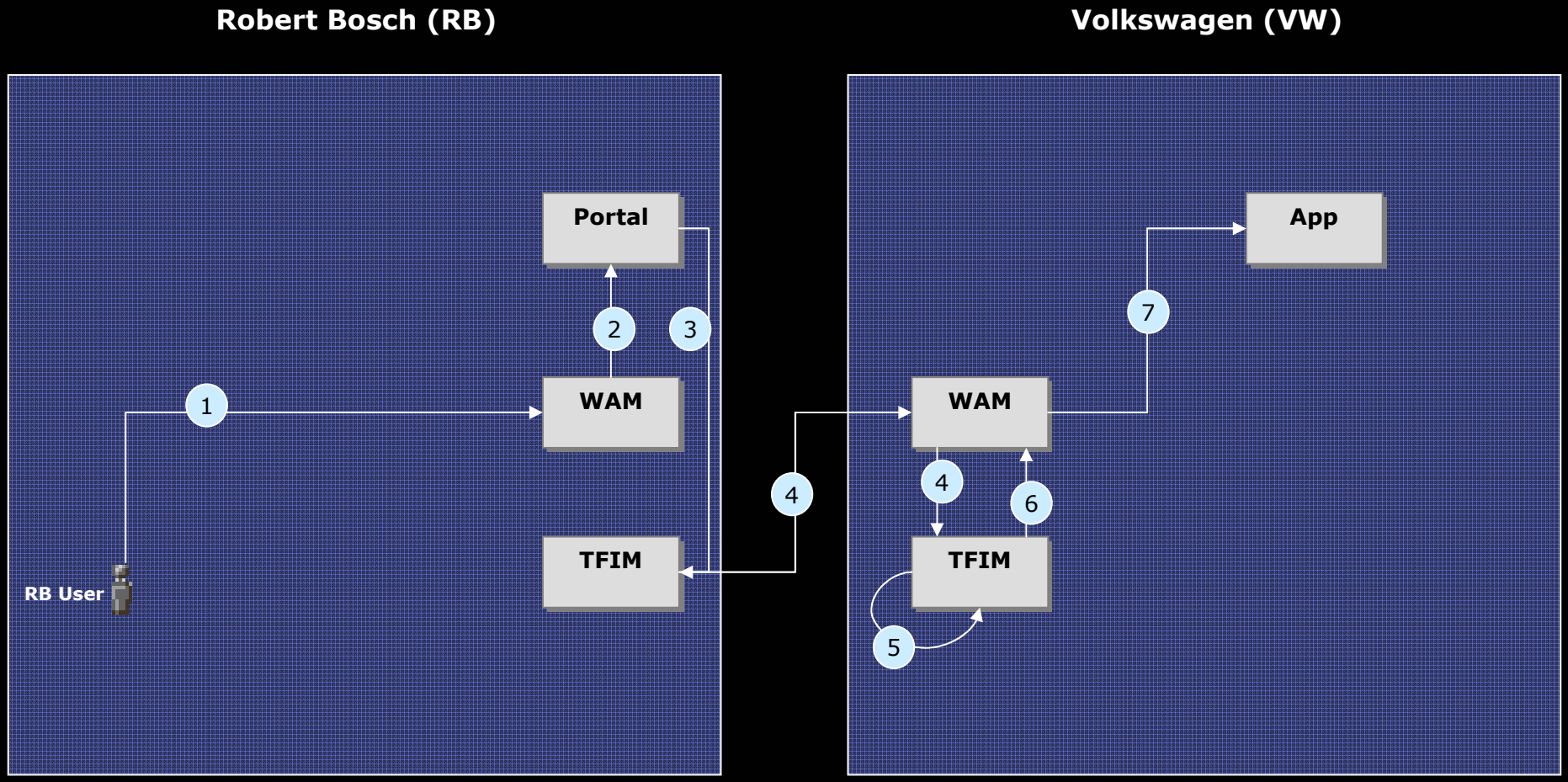
UK Government

- UK Government Gateway/Connect
  - Acts as an IdP
  - Local authorities act as SP
    - e.g. Hampshire County Council (HCC)
  - WS-Federation
    - SAML tokens
  - TFIM used at SP (HCC)
    - Solution extended to support upload of know facts (registration process)

Manufacturing (Automotive)

- VW and Bosch Use Case
  - Federation within the supply chain
  - Fed SSO from Bosch to VW
    - WS-Fed (SAML token)
- Bosch employees need to access VW application
  - Application
    - system for VW´s development and design department
- Today VW have to provide Bosch employees id's an manage their passwords for access
- Federation enables them to exploit a more efficient trust model

Fed SSO (IdP initiated)



(1) User authenticates at RB WAM

(2) User is directed to RB Portal

(3) User clicks SSO link to VW Application. That causes TFIM to generate an HTML form with the SAML assertion and target URL included

(4) The form is sent to VW via scripted POST

(5) TFIMs Assertion Consumer Service receives POST. Assertion is decoded and validated.

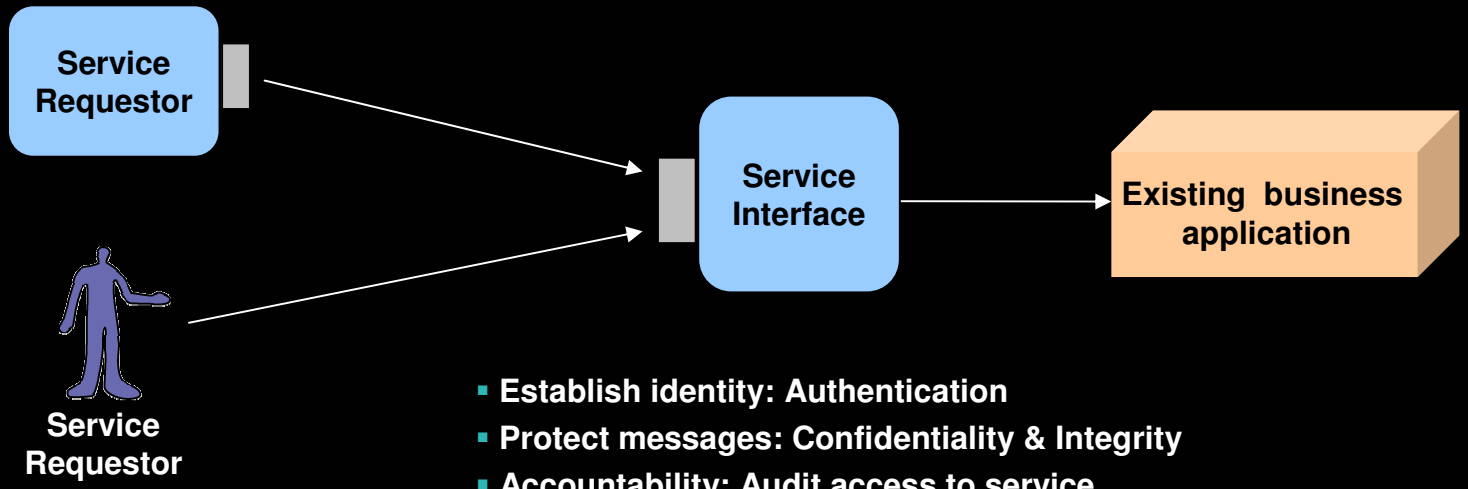
(6) TFIM builds an authenticated session for user

(7) User is redirected to target URL (Application)

Security Considerations for SOA

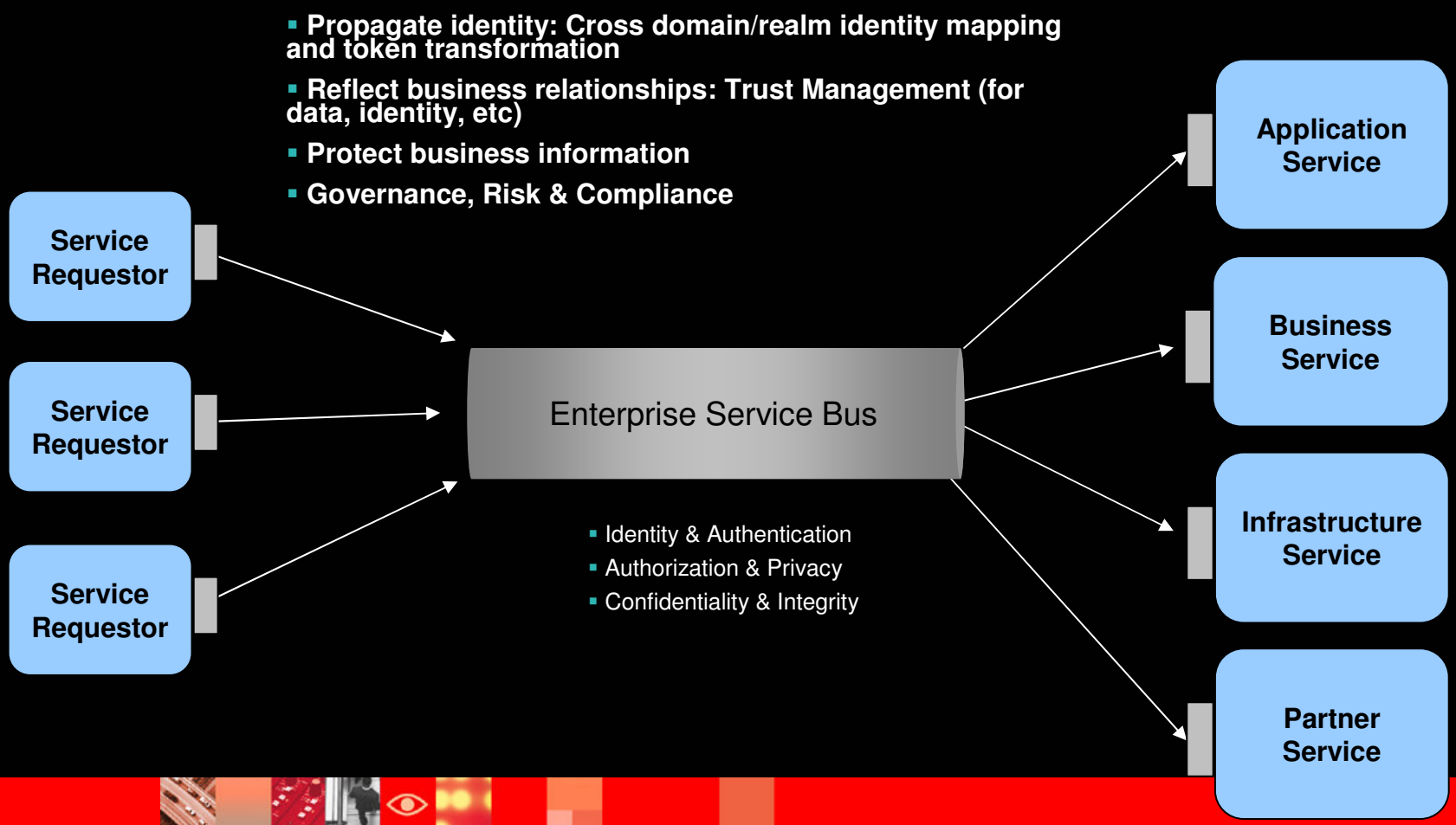
- Entities/Identities – users, services
  - Services have identities
  - Identities and/or credentials are propagated across services
  - Users and services are now subject to the same security controls
- Organizational/enterprise boundaries
  - Perimeter is obscure
  - Identities are managed across boundaries
  - Trust relationships are established across boundaries
- Composite applications
  - Ensuring proper security controls are enacted for each service and when used in combination
- Greater focus on data/information
  - Protecting data at transit and at rest
  - Apply consistent protection measures
  - Access to data by applications and services
- Governance, Risk, and Compliance
  - Auditing ie. entity identification to specific transactions

Use Case 1 - Service Creation



- Establish identity: Authentication
- Protect messages: Confidentiality & Integrity
- Accountability: Audit access to service
- User experience: SSO, Privacy

Use Case2 – Services Integration



Use Case 3 – Service Aggregation for Collaboration

-**Provide access to business services through a common interface, ie portal.**

-**Simplify the user's interaction with the security services via SSO**

-**Meet audit requirements with user's identity propagated to all application components, ie no service accounts**

Service Requestor

Pervasive Access

Portal & Collaboration

- **Identity & Access**
- **Trust Management**
- **Governance, Risk & Compliance**

Enterprise Service Bus

- Identity & Authentication
- Single Sign-On (Web and Federated)
- Self-Care, Profile Mgmt.

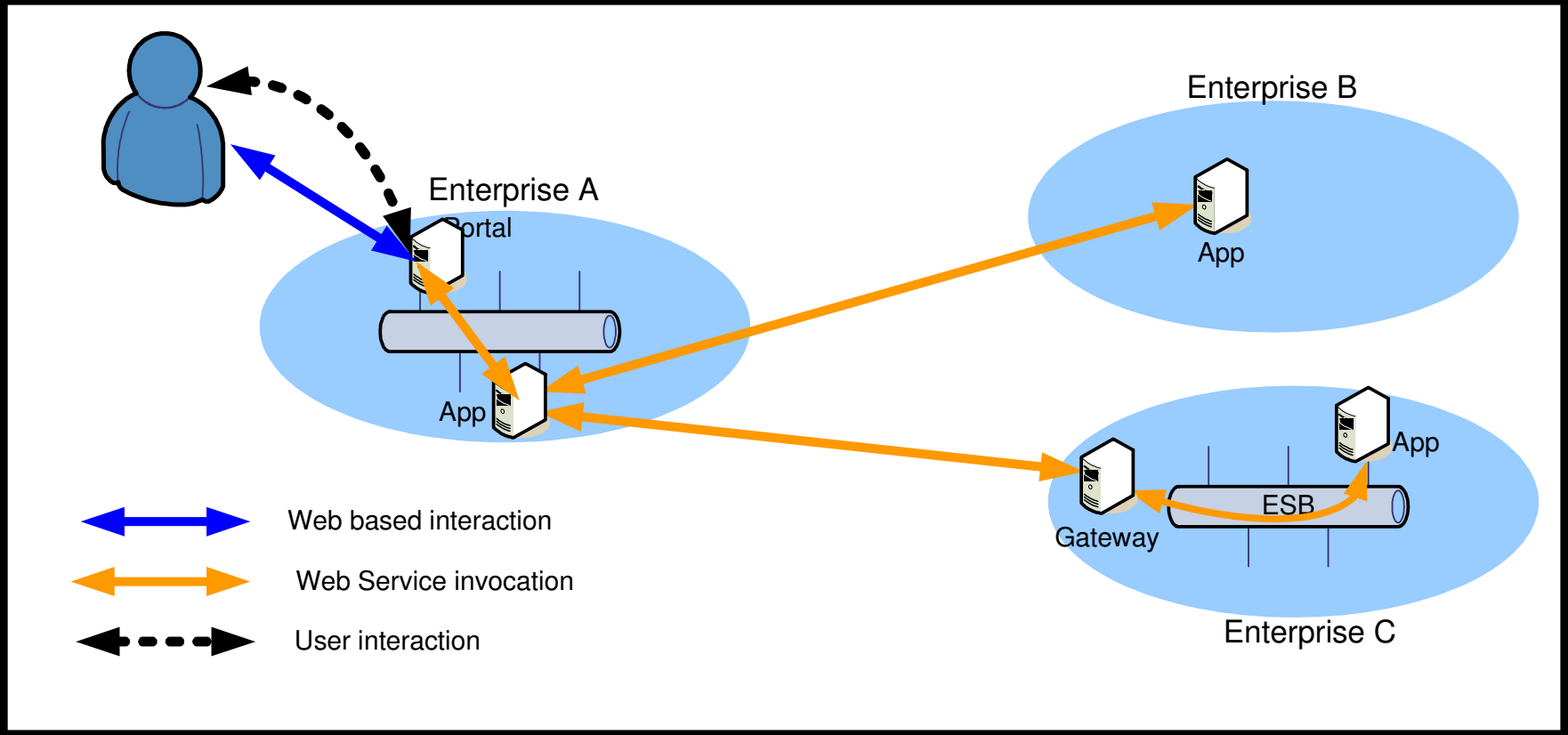
Application Service

Remote Portlets (WSRP)

Partner Service

Partner Service

Federated Web Services



- **Key security requirements for both inbound & outbound requests:**
  - Security Token Mapping
  - Identity Mapping

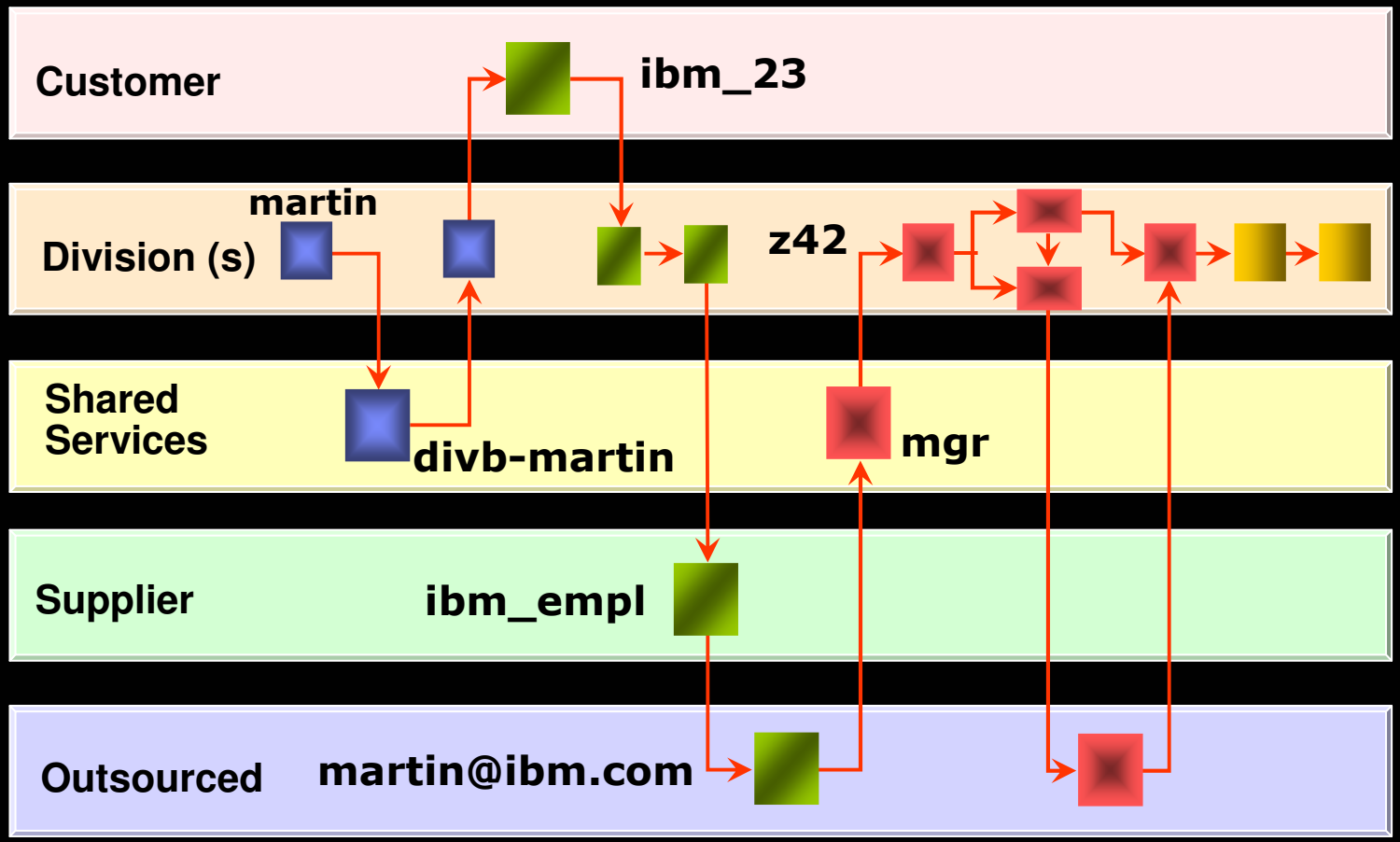
What does IBM Tivoli Federated Identity Manager (TFIM) bring to table?

- Ability to handle identity/attribute transformation as part of token handling
- Ability to exchange token types as part of validation of request at edge
  - Enables advanced “intermediary” type functionality
- Ability to do authorization decisions at abstract WSDL level
  - Independent of WSDL binding
- Integrates with TAM Authorization
  - Access allowed? (Yes/No)
  - Protected Object Policies (e.g. Time of Day)
  - Authorization Rules (authorization policies based on client attributes)
- Audit
- All of this in a standards-based manner!

WS-Trust : Overview

- WS-Trust defines mechanism for:
  - "…security token exchange to enable the issuance and dissemination of credentials within different trust domains"
- Defines the *Security Token Service (STS):*
  - Request security tokens
  - Validate security tokens
  - Exchange security tokens
- The TFIM STS provides:
  - Token mediation (validation, mapping, issuance)
  - Identity mediation
  - Authorization (via TAM)
  - Auditing (to CARS)

Identity Flow in a Service Oriented Architecture



IBM Security Solutions Continue to be Recognized for Leadership

- #1 Provisioning and Web SSO Vendor, IDC (July 2007)
- Gartner Leadership Quadrant, Web Access Management (September 2006)
- Gartner Leadership Quadrant, User Provisioning (April 2006)
- Gartner Leadership Quadrant, Web Services (2005)
- #1 Provisioning and Web SSO Vendor, IDC (August 2005)
- Information Security Names IBM Tivoli to The Influence List for 2003-2008
- 2005 #1 Provisioning Vendor, Gartner Vendor Selection Tool
- 2005 Frost & Sullivan Global Market Leadership Award for Identity Management
- 2004 SYS-CON Best Web Services Security Solution Award
- 2004 Information Security Product-of-the-Year Bronze Award for Authentication and Authorization
- 2003 Frost & Sullivan Market Engineering Leadership Award
- 2003 Crossroads A-List Award for Integrated Identity Management Solution
- 2003 Network Computing Well-Connected Award Finalist
- 2003 SC Magazine Reader Trust Awards – Best General Security Finalist
- 2003 LinuxWorld Product Excellence Award – Best Security Solution Finalist
- 2003 Top WLAN Companies of the Year for Leadership in Wireless Security
- IBM Tivoli Access Manager Sets New Performance Records – Mindcraft Benchmark
- IBM Tivoli Wins Information Security Excellence Award for Second Year in a Row
- 2002 Information World Editor's Choice Award for Security Software