Securing a Federated SOA
A government case study in using security to enable a Service Oriented Architecture (SOA) federation

John Sullivan
Security Architect, Advanced Technologies Group

Session Objectives

By the end of this session,
you will be able to:

- Describe the business requirements leading to a federated SOA
- Create the end to end security architecture for a federated SOA
- Be able to apply IBM technology from WebSphere and Tivoli in the implementation

Agenda

Topics

- Current SOA Projects
- SOA Projects
- Case Study: MCIT GSB Project
- MCIT GSB Security
- Conclusions
- Pass it On!

Current SOA Projects

What type of projects are common today?

Current SOA Projects
Focused on the enterprise

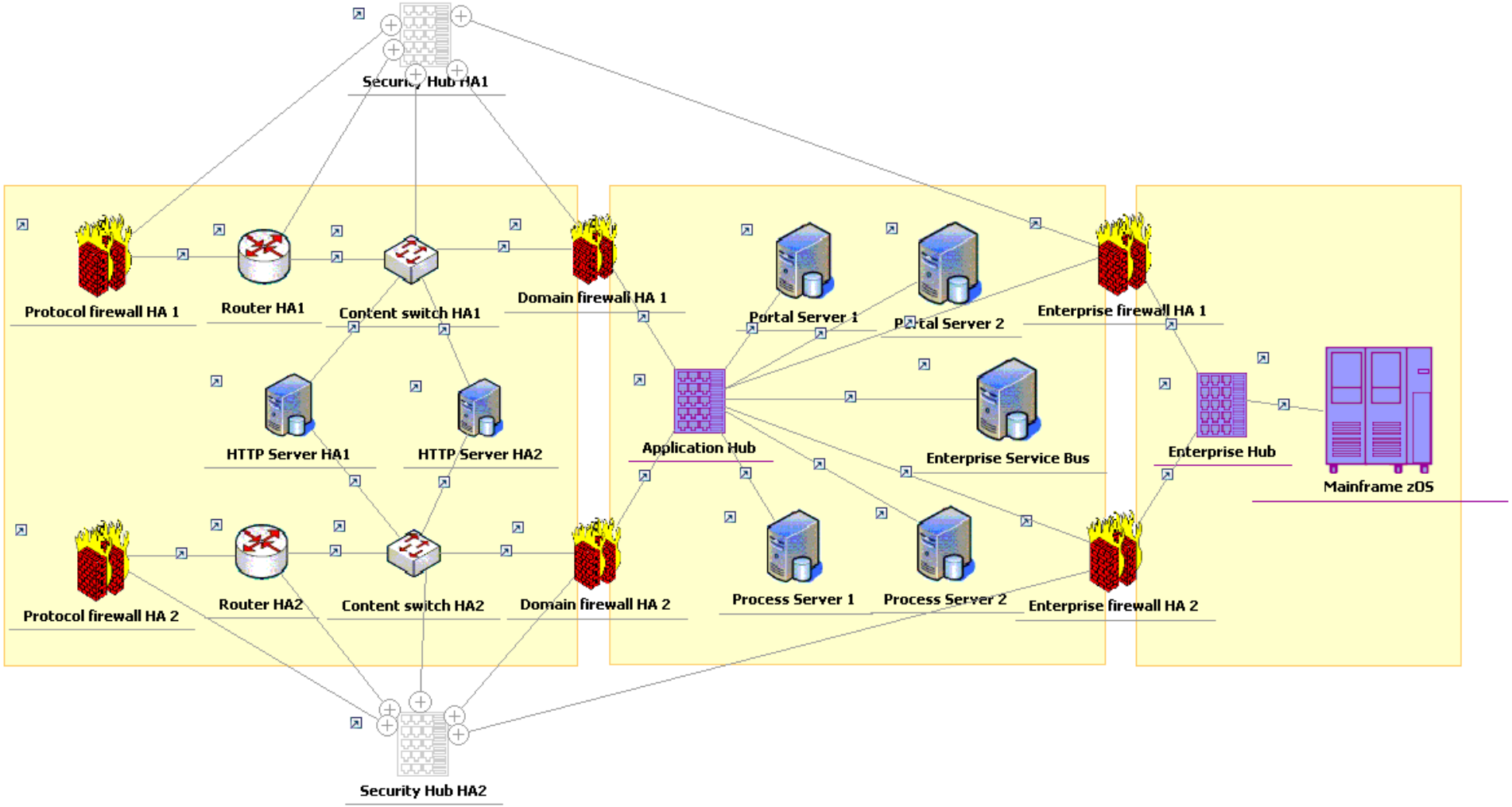
- Goal
  - SOA enablement of the enterprise
- SOA entry points
  - Re-use – service creation
  - Connectivity – service connectivity
  - People – interaction and collaboration services
  - Process – business process management (most popular)
  - Information – information as a service
- SOA disciplines
  - Governance
  - Security and Management
  - Design
  - Test
- See https://w3.webahead.ibm.com/w3ki/display/SOAScenes/Home

Current SOA Projects
Focused on the enterprise

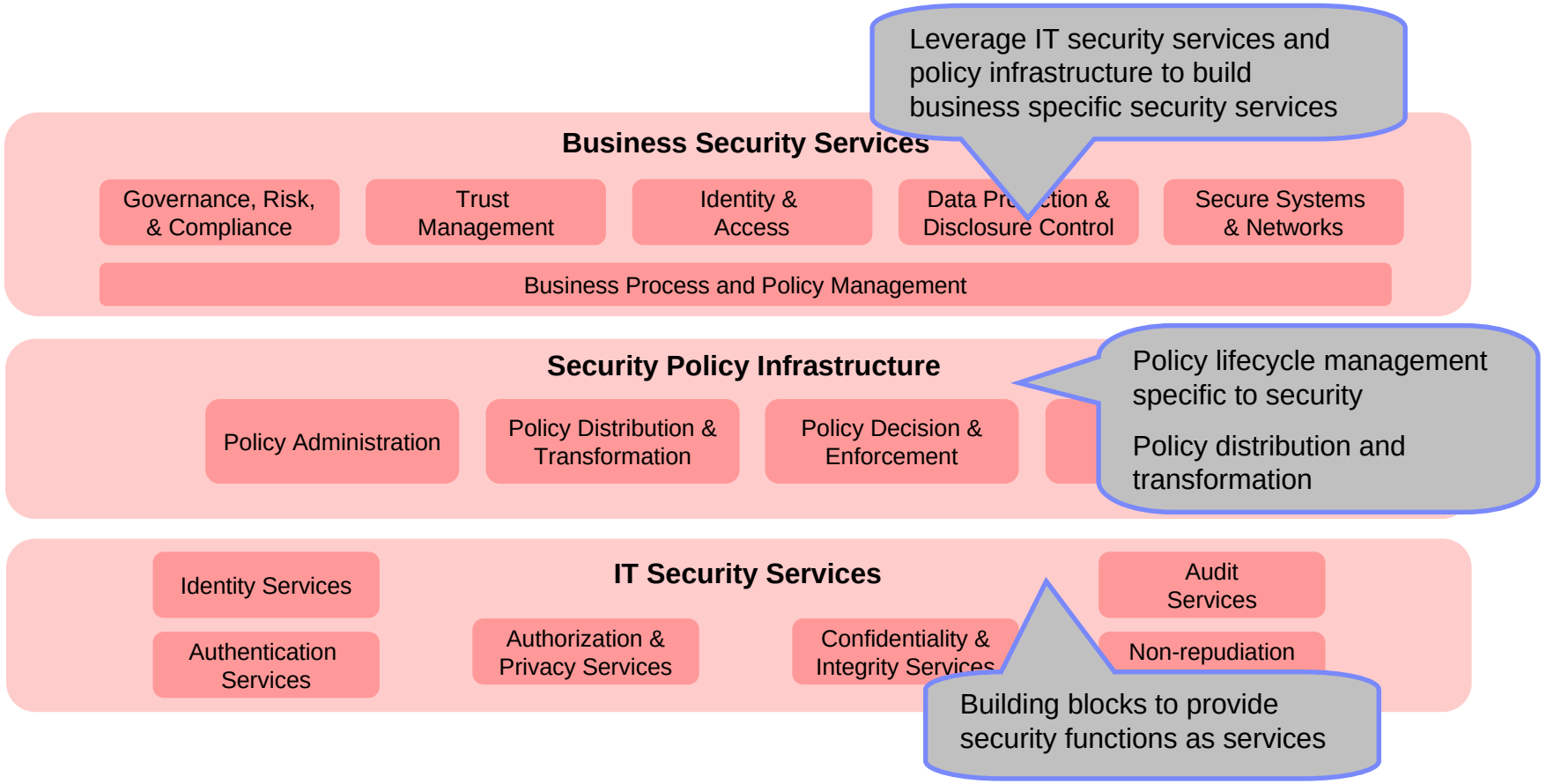
- Some external interactions with third parties
  - Users (browser based)
  - Service Consumers (web services)
  - Service Providers (web services)

- In general these external interactions have been limited when compared with the larger enterprise SOA enablement goal

Current SOA Projects
Sample Architecture

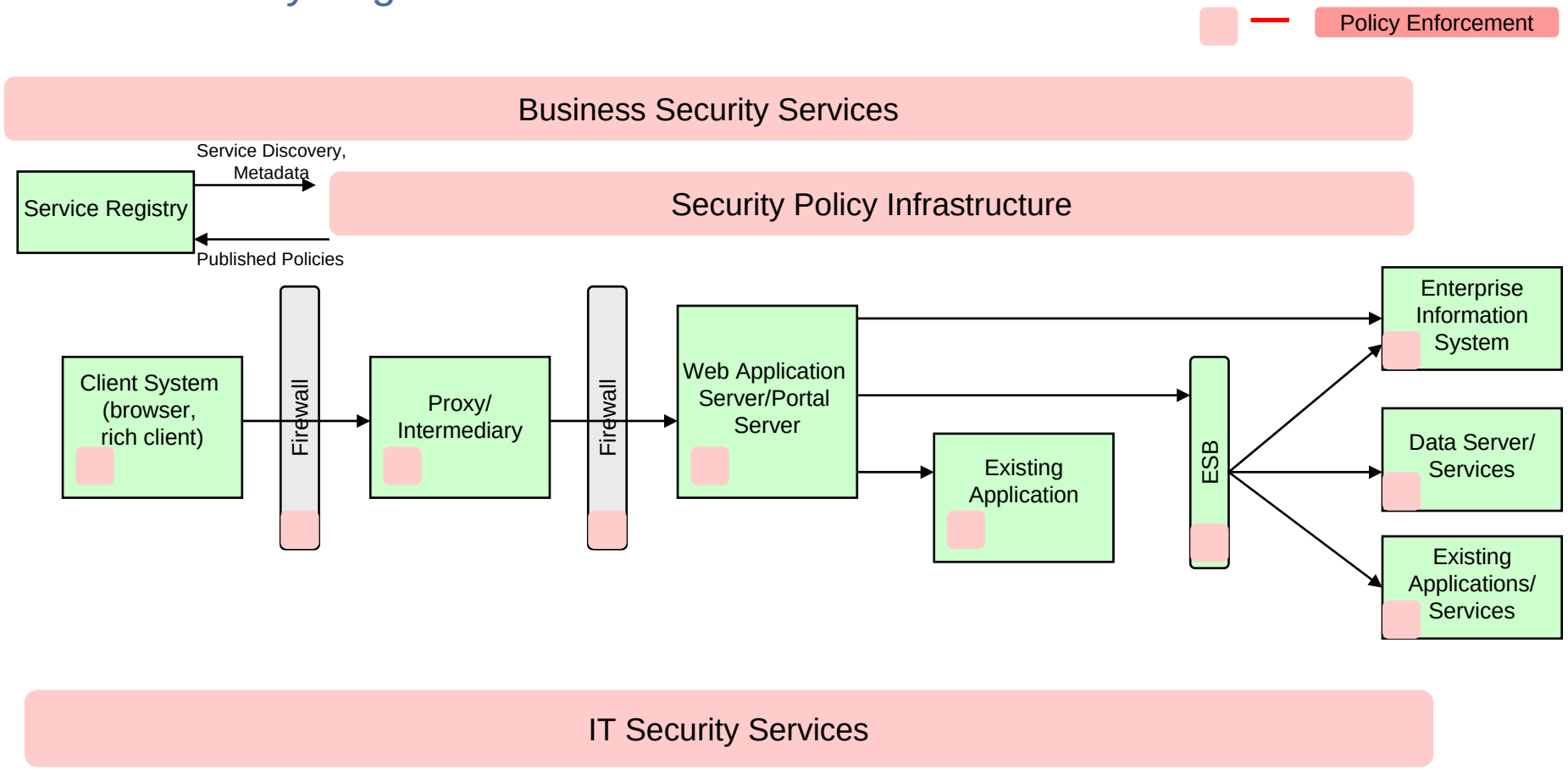


SOA Security – Reference Model



8

SOA Security Logical Architecture



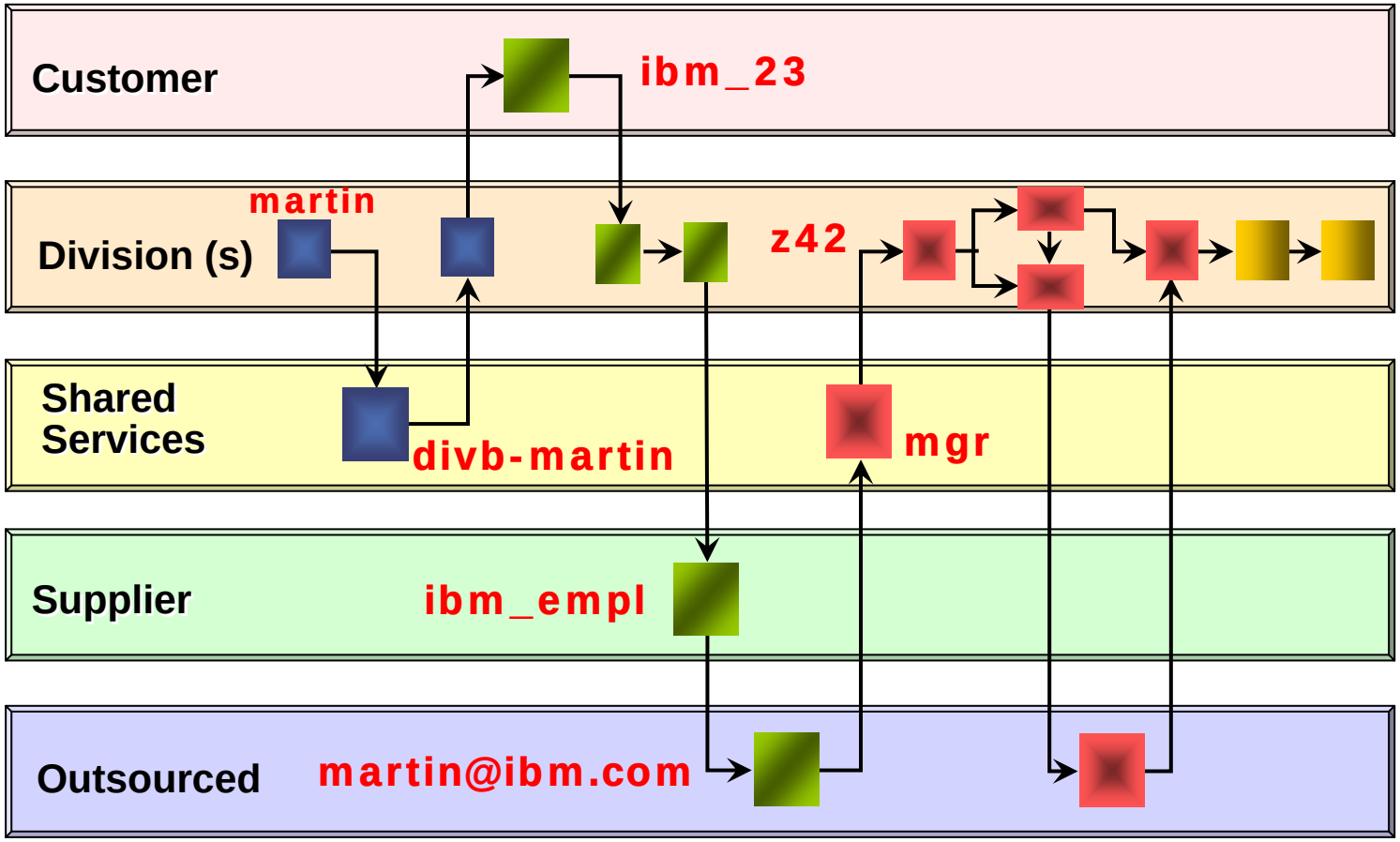
Policies are distributed to not only to Security Services but only to different enforcement points.

The Enforcement points can leverage local capabilities or access centralized security services to enforce policies.

9

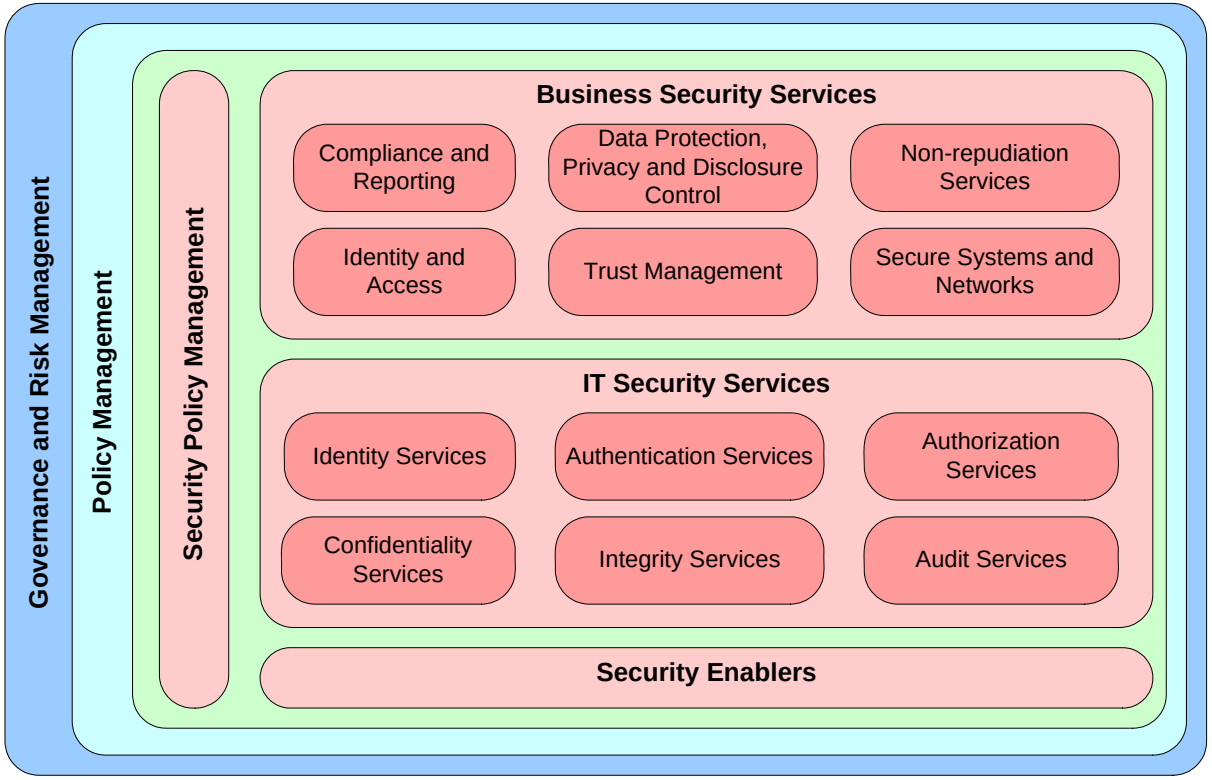
Identity Flow in a Service Oriented Architecture

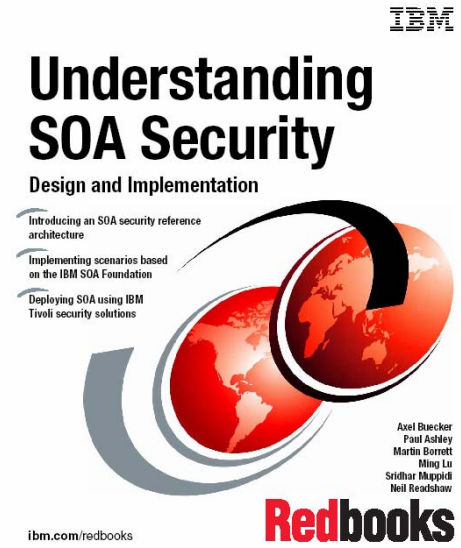
How does Identity flow between services ?



10

Current SOA Projects
SOA Security Maturity





- At various speeds, enterprises are moving to a higher level of SOA maturity
- SOA security is also maturing

Current SOA Projects
SOA Security products

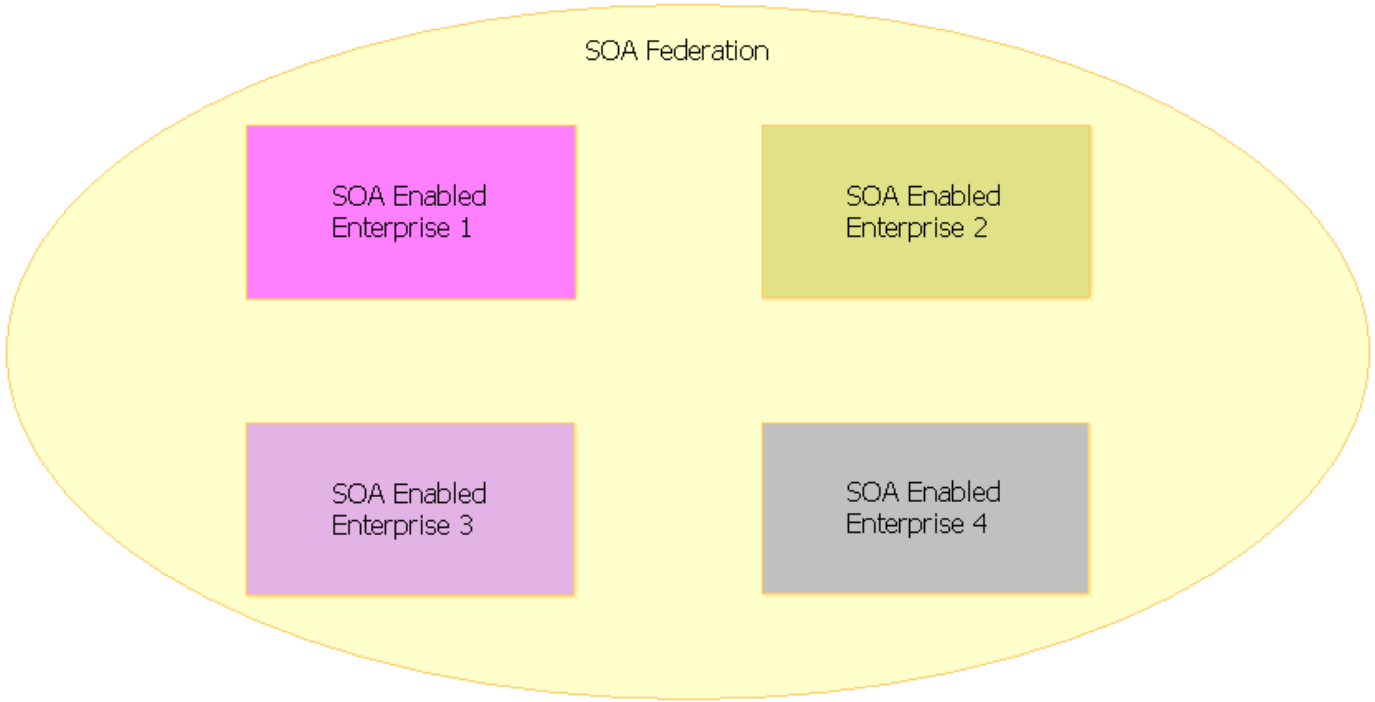
- Very common in SOA projects:
  - Tivoli Access Manager for e-business (TAMeb)
    - Web single sign-on
  - Tivoli Federated Identity Manager (TFIM)
    - Security Token Service for backend integration
  - Tivoli Identity Manager (TIM)
    - Managing the lifecycle of internal users
  - Tivoli Directory Server (TDS)
    - Storing the user identity data
  - WebSphere DataPower XS40 Appliance
    - Providing a web services gateway for connecting to other parties

SOA Projects

A new style of project is emerging – federations of SOA enabled enterprises

SOA Projects
Federations

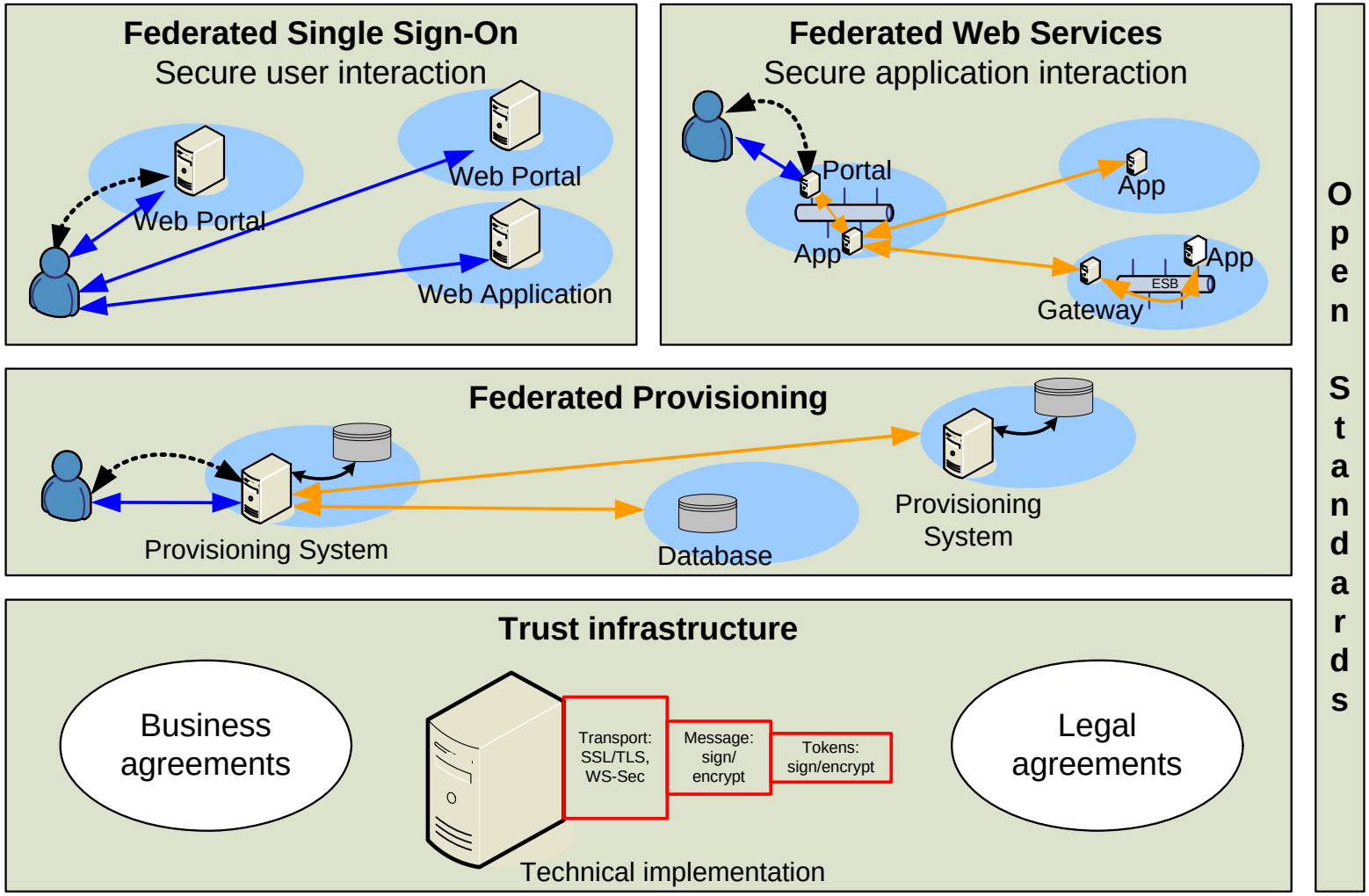
- The discussion among these SOA enabled enterprises is changing
  - *how can we now work together to improve the usability and lower our operating costs?*
  - *how can we leverage each others services?*
- Answer: SOA federation



SOA Projects
Federations (cont.)

- SOA federation projects are focused in two main areas:
  - The enterprises can leverage each others business services as part of a composite application
    - Services federation
  - Providing single sign-on across the web sites of the enterprises
    - Federated web single sign-on
- I would classify projects that are implementing **both** areas as SOA federation projects.
- Surprisingly, projects in the **government sector** are leading the way

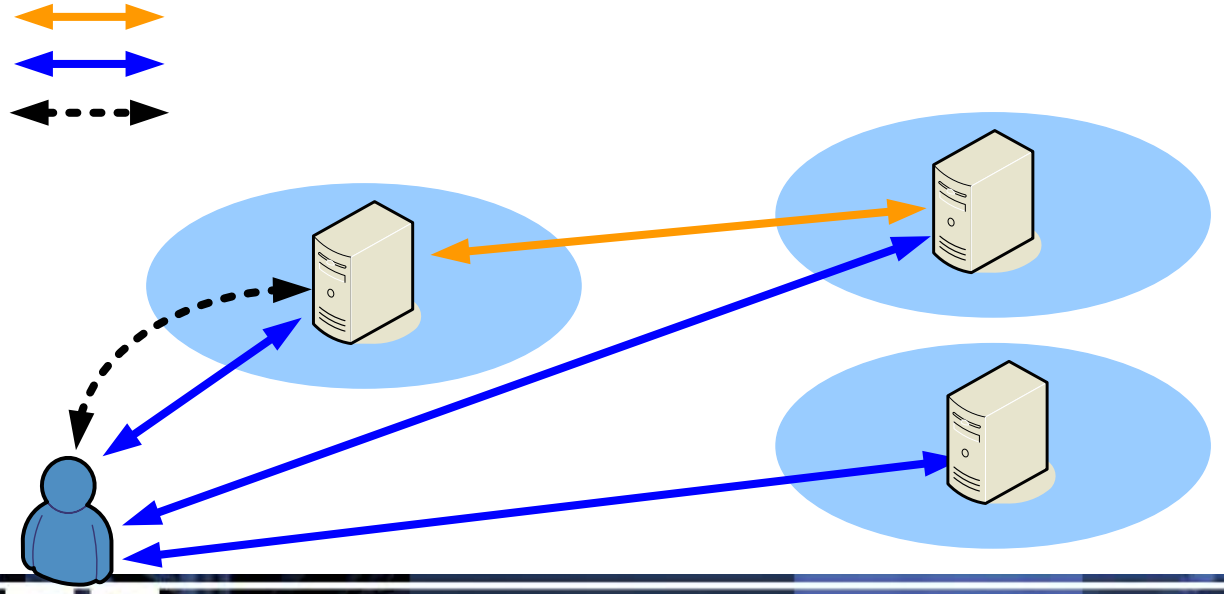
SOA Projects
Federation Requirements



SOA Projects

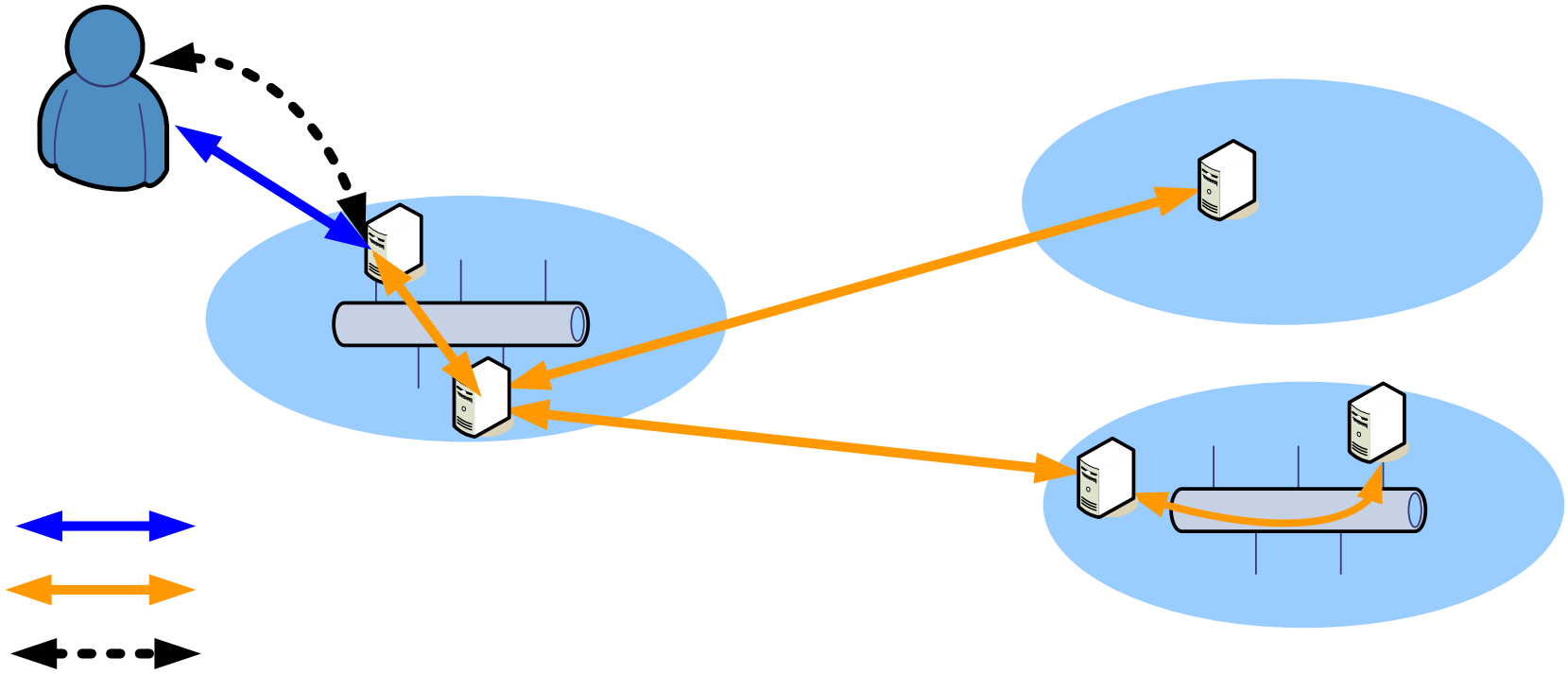
Federated Web Single Sign-On

- **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.
- **SAML, Liberty ID-FF, WS-Federation**



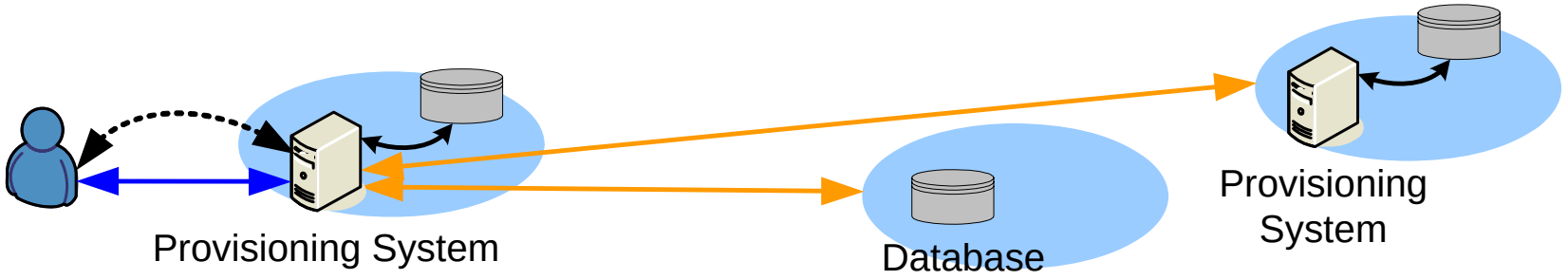
SOA Project
Federated Web Services

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



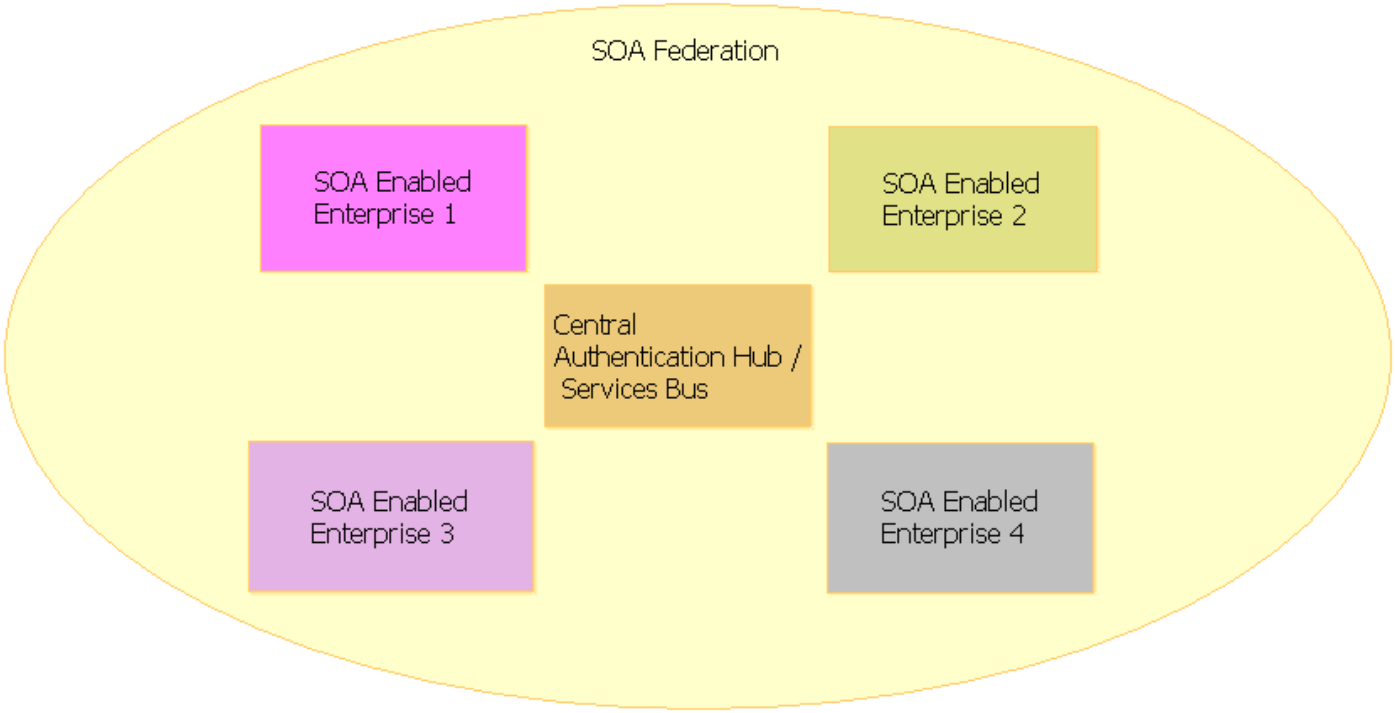
SOA Project
Federated Provisioning

- Current deployments typically involve non real-time solutions for provisioning
  - E.g. weekly tapes, daily ftp of files.
- New business models will require closer to real-time provisioning and just-in-time provisioning solutions
- Uptake of the federated provisioning standards has been slower
  - **WS-Provisioning / WS-Notification**
  - **SPML v2.0**
  - **Liberty**



SOA Projects
SOA Federation Architecture Pattern

- The current **pattern** identified is to build
  - A centralized services bus that coordinates the services provided by each of the enterprises
  - A centralized authentication hub that authenticates users and provides single sign-on tokens



Case Study: MCIT GSB Project (Minister of Communication & IT Government Service Bus)

A federation of SOA enabled government agencies and third parties

Case Study: MCIT GSB Project
Project Overview

- The Yesser e-government program is aimed at the ease and speed of interaction for
  - Government to Government (G2G)
  - Government to Citizen (G2C)
  - Government to Business (G2B)
  - http://www.yesser.gov.sa/english/default.asp

- **IBM's project is to build the Government Services Bus (GSB)**

- Project in Riyadh, Kingdom of Saudi Arabia

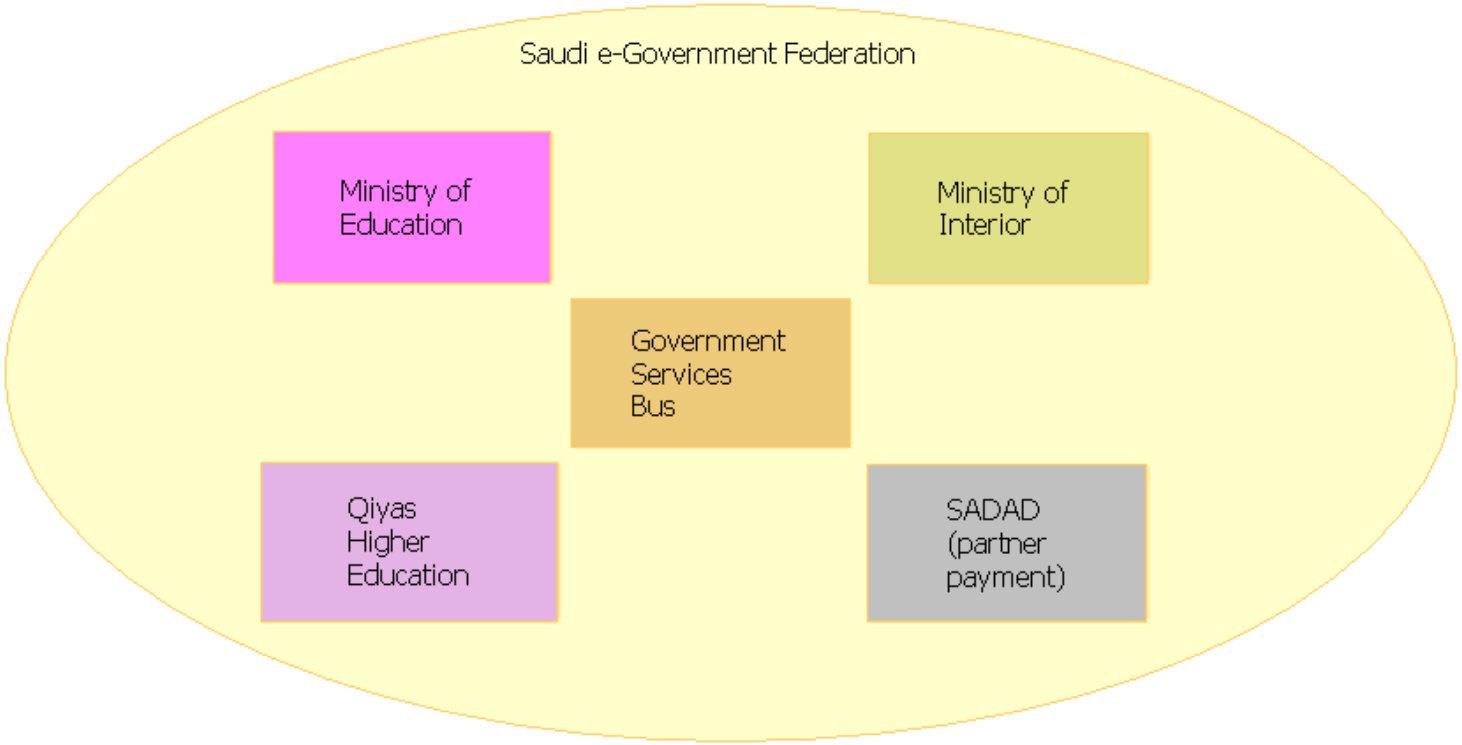
Case Study: MCIT GSB Project
From the RFP

- *The Government Service Bus (GSB) is the set of all elements that constitute a Service Oriented Architecture (SOA)-enabling infrastructure.*
- *Its main role is promoting loosely-coupled, highly-centralized services that are seamlessly integrate-able.*
- *The GSB provides an infrastructure that removes any direct connection between service consumers and providers.*
- *Consumers connect to the bus and not the provider that actually implements the service. This provides location independence to all services.*
- *The GSB also implements further value add Infrastructure or "Fabric"services.*
  - *security, transaction, scalability, directory, registry and delivery assurance are implemented centrally within the bus instead of having these buried within the applications or at the government agency back-ends*

Case Study: MCIT GSB Project

Phase 1

- Phase 1 includes four federation partners
  - Three agencies and one third party
  - 6 use cases
  - Scheduled for production in May
- End system will involve more than 20 agencies and numerous third parties



MCIT GSB Security

Building secure federation capabilities

MCIT GSB Security
From the RFP - Security

- *Users identity and credentials (user id, password, group information etc) will be stored and managed in the GSB LDAP directory. This LDAP directory will contain users aggregated from all the agencies portals.*
- *A web single sign on capability between participating government agency web sites and GSB is required. A solution is to use SAML Browser Artifact Profile.*
- *Transmission security of data is required between government agencies and the GSB and between other service providers and consumers of the GSB.*
- *Secure network access to the GSB via appropriate security mechanisms must be provided, e.g., firewall, remote access gateway.*
- *The proposed solution must be built using products, hardware and software that readily allow clustering, disaster recovery and load balancing.*
- *Standards based approach using WS-Security, WS-Trust*
- *Audit and Reporting on security events across the environment*

MCIT GSB Security
Main security use cases

1.Authentication to e-Portal at the GSB

- Initially 2.6 million users (10% of population growing 30% per year)

2.Federated Web single sign-on

- GSB acting as SAML Identity Provider
- Agencies acting as SAML Service Provider
  - Will need SAML capabilities but technology not mandated

3.Web Services security

- Edge Gateway
  - XML validation, WS-Security, WS-Trust
- Identity Propagation end to end
  - WS-Security tokens

MCIT GSB Security
Main security use cases (cont.)

4.Identity Lifecycle Management

- Management of millions of Internet based users
  - Federated provisioning across the federation
- Management for GSB internal people
  - OS admins, Application Server admins, Database admins …

5.Security Auditing and Reporting

- Collect security logs across the environment
- Normalize these, store in database
- Report on them

6.PKI Integration

- Separate PKI project
- Must ensure that IBM components can operate with certificates and keys generated

MCIT GSB Security
Key Architectural Decisions

1. Use point of contact servers in a DMZ environment for all in-coming and out-going transactions to/from the GSB
   - Use hardware appliances for dealing with web services messages

2. Provide authorization at every layer in the architecture
   - Course grained at the point of contact servers
   - Increasing more fine grained towards the back-end systems

3. Use only a standards based interconnections
   - Web Services
     - WS-Security
     - WS-Trust
     - SAML
     - WS-I Basic Security Profile

MCIT GSB Security
Key Architectural Decisions (cont.)

4. Use SSL in combination with WS-Security
   - Use WS-Security only for carrying security token
   - **Exception** is requirement for end to end protection

5. Use SAML 2.0 Browser Artifact Profile for Federated web single sign-on

6. Use SAML 1.1 assertions with WS-Security for service requests/replies to/from the GSB

7. Use Username tokens within the GSB where possible
   - May need to use SAML assertions in some cases

MCIT GSB Security
Key Architectural Decisions (cont.)

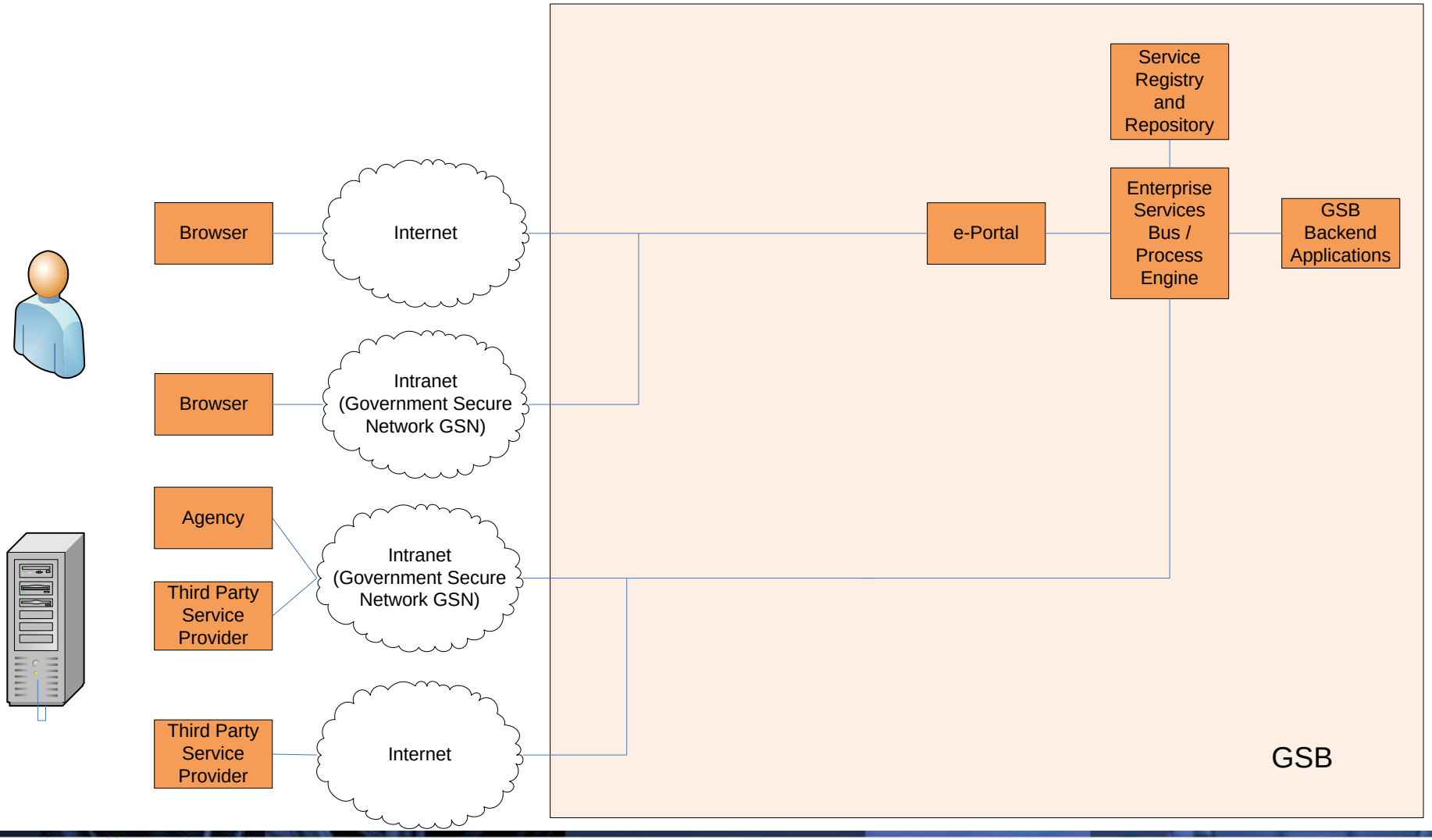
8. Use TFIM as the Security Token Service for the edge gateway.
   - More flexible and better configuration

9. Use ‘out of the box’ products with as little custom development as possible
   - Low risk and cost
   - Highly available and scalable configurations

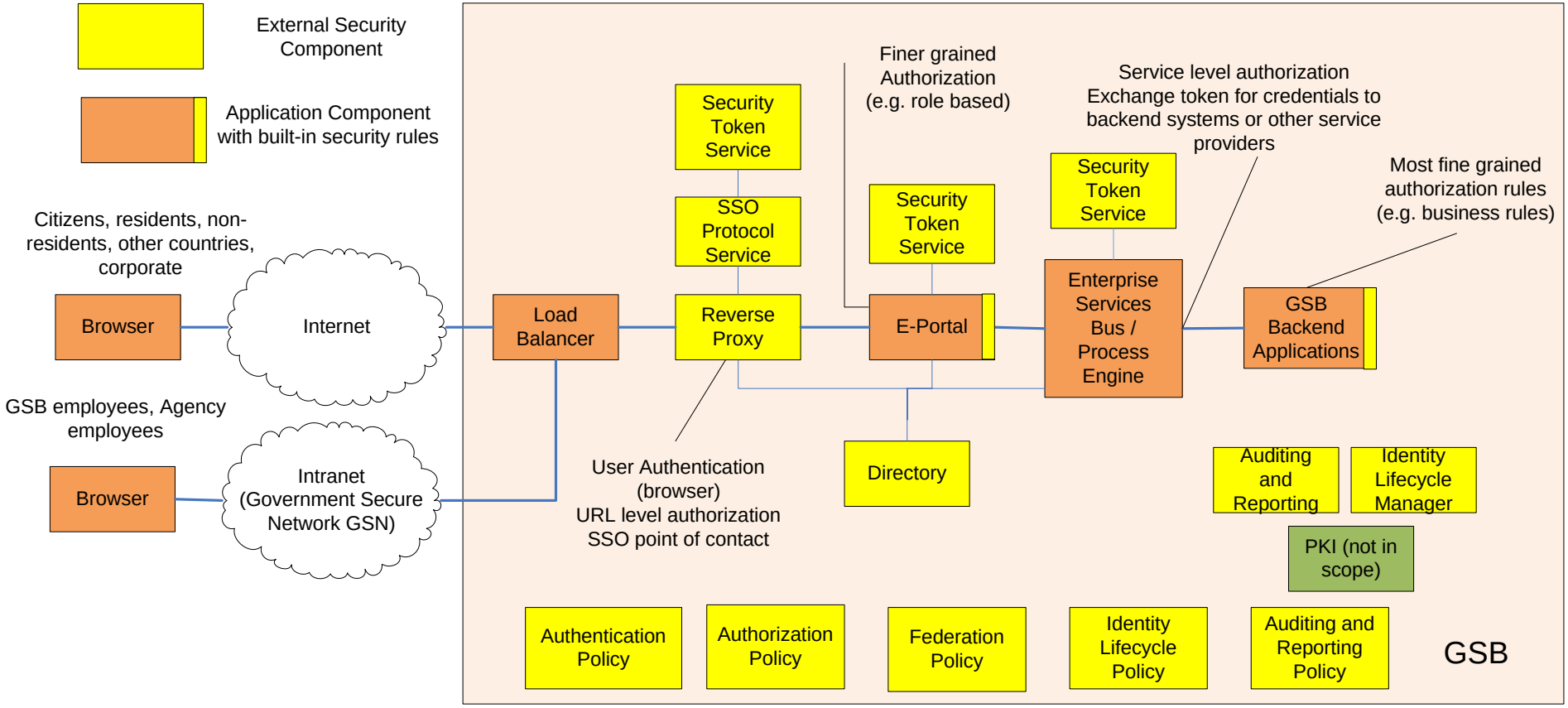
10. Only use security architectural patterns that have been proven at other IBM client environments

MCIT GSB Security

GSB - Conceptual Web and Web Services

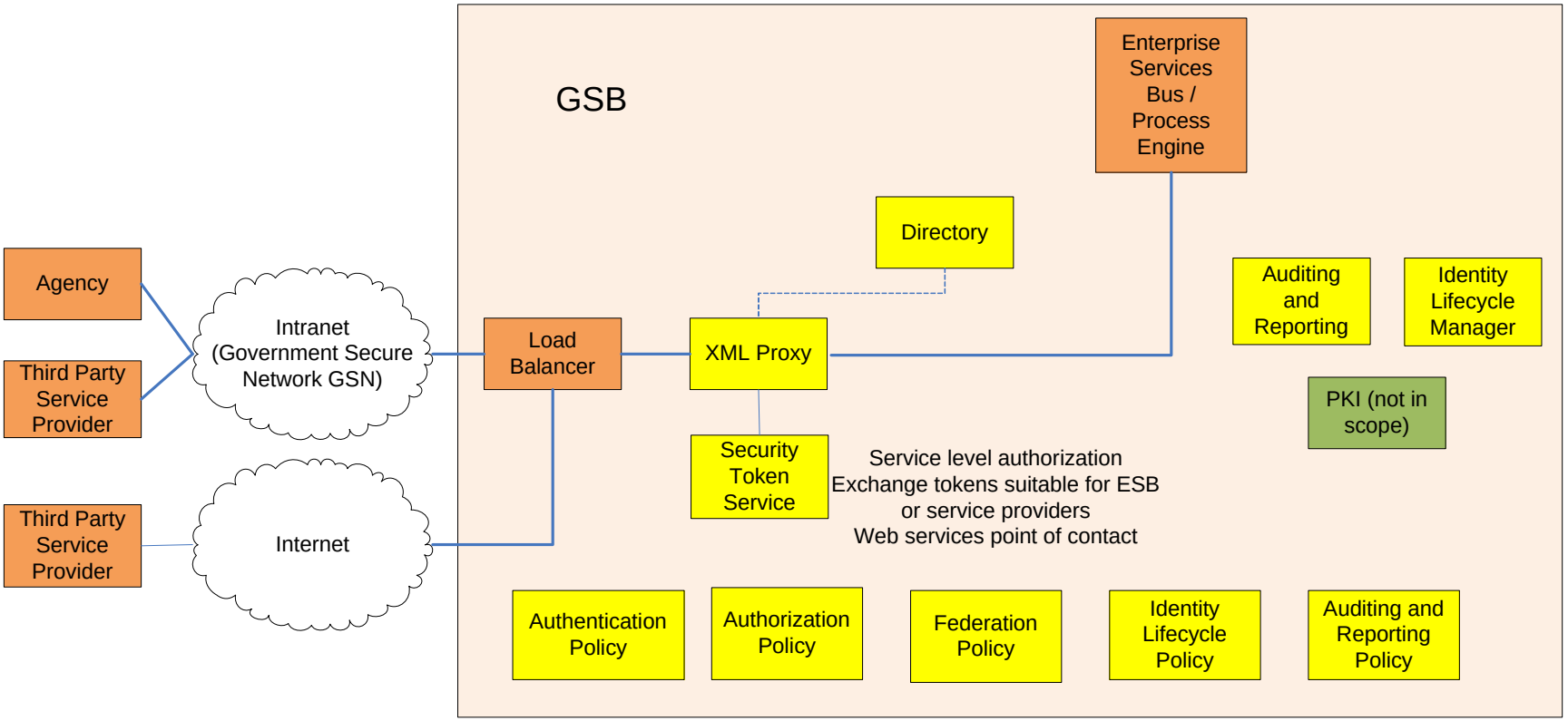


MCIT GSB Security
GSB - Conceptual Web security



MCIT GSB Security

GSB - Conceptual Web Services security



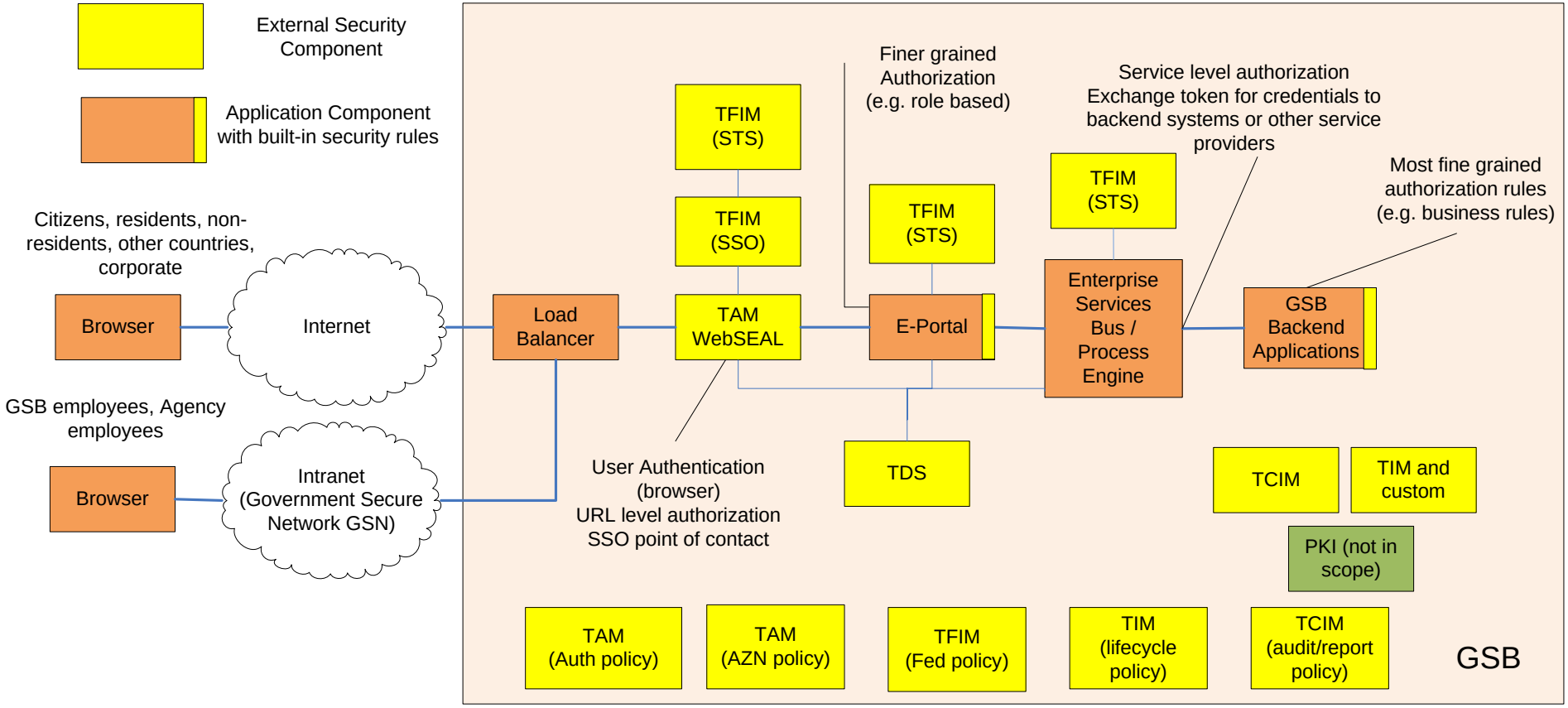
See also

http://www-128.ibm.com/developerworks/websphere/techjournal/0603_col_hines/0603_col_hines.html

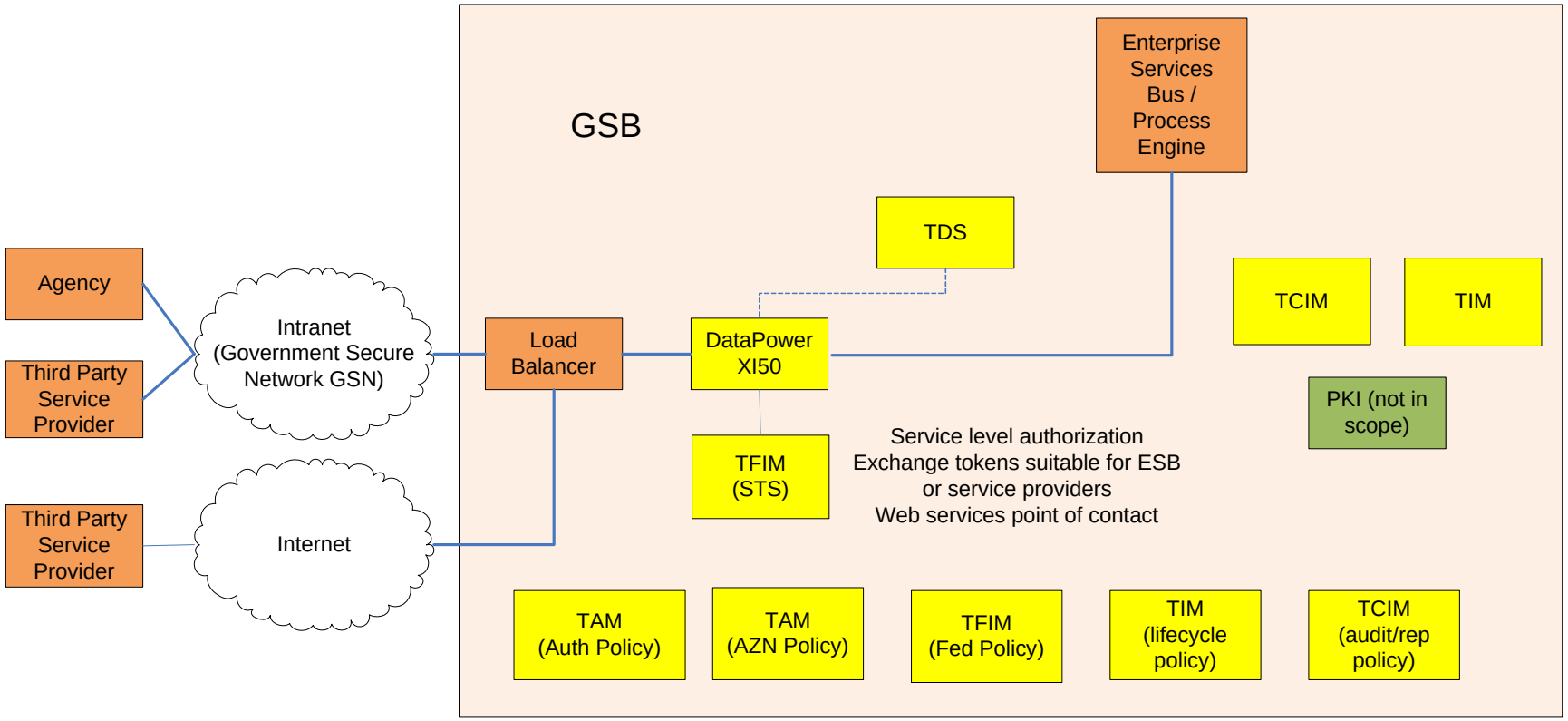
MCIT GSB Security
GSB – Security Products

- Tivoli Federated Identity Manager (TFIM)
  - Federated Web Single Sign-On
  - Web services security Security Token Service
- Tivoli Access Manager for e-business (TAM)
  - Authentication / Authorization Policy
  - Web point of contact
- WebSphere DataPower XI50
  - Web Services point of contact
- Tivoli Identity Manager (TIM)
  - User lifecycle management (initially internal users only)
- Tivoli Compliance Insight Manager (TCIM)
  - Collating, storing and reporting on security events
- Tivoli Directory Server (TDS) / Tivoli Directory Integrator (TDI)
  - Managing millions of identities
  - Provide synchronization capabilities

MCIT GSB Security
GSB - Web security (products)



MCIT GSB Security
GSB - Web Services security (products)



Conclusion

Security is the key enabling technology for SOA federations

- Centralized hub for service invocations and federated web single sign-on the current popular architectural pattern
- Tivoli and WebSphere products can be used to build the hub

Resources

- Understanding SOA Security Design and Implementation
  - http://www.redbooks.ibm.com/redpieces/abstracts/sg247310.html
- Propagating Identity in SOA with IBM Tivoli Federated Identity Manager
  - http://www.redbooks.ibm.com/redpieces/abstracts/redp4354.html?Open
- SOA Security and Management (Scenario 7) Portal
  - http://publib.boulder.ibm.com/infocenter/soasdbox/v1r0m0/index.jsp?topic=/com.ibm.soln.SOASandboxConfigs.nav.fw.doc/home_pages/welcomeSecMgmt.html
- Federated Identity and Trust Management
  - Redpaper and Redbooks at:
    http://www.rebooks.ibm.com/

Review of Objectives

Now that you've completed this session, you are able to:

- Describe the business requirements leading to a federated SOA
- Create the end to end security architecture for a federated SOA
- Be able to apply IBM technology from WebSphere and Tivoli in the implementation

Pass it on!

Three things to remember and why they are important to share

- SOA federations are partnerships of SOA enabled enterprises
- Security is the key enabler to support the SOA federations
- The MCIT case study demonstrates IBM has experience in securing these environments


Thank
You

Backup Slides

Kingdom of Saudi Arabia

Transforming citizen services to improve quality of life

The Need:

With most government processes delivered manually, agency staff found it could take days and weeks to respond to citizen inquiries. The Kingdom of Saudi Arabia sought to replace these cumbersome, time-consuming processes, with anytime, anywhere services that would improve its interaction with citizens.

The Solution:

Working with IBM and IBM Business Partner Saudi Business Machines, the Kingdom of Saudi Arabia implemented a new communication and security infrastructure that automates business processes, increases agency collaboration and provides citizens with online, voice and mobile device access to government services. Based on a service oriented architecture, nearly 1,000 processes, including unemployment services, work permits and government payments will be deployed as anywhere, anytime electronic services.

What Makes it Smarter:

- Fundamentally transforms the interaction between the Saudi government and the people to help to improve quality of life for citizens
- Anywhere, anytime access enables government to reduce response time from several days to minutes
- Greater collaboration improves efficiency of government agencies and increases staff productivity

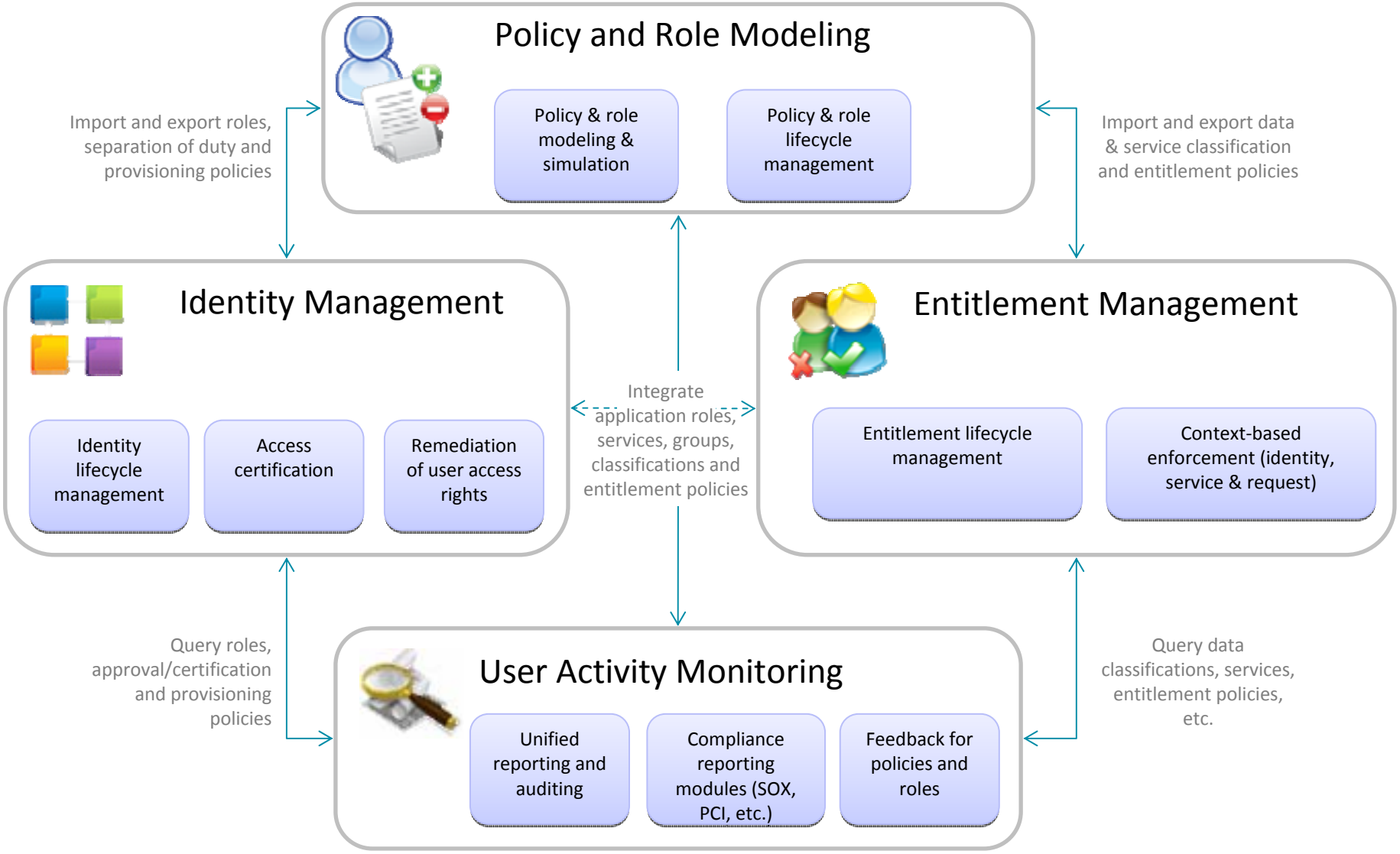
"IBM is helping us realize our vision for smarter government, dramatically simplifying citizens' interactions with government agencies while increasing overall efficiency."

— Name, Title, Kingdom of Saudi Arabia

Solution components:

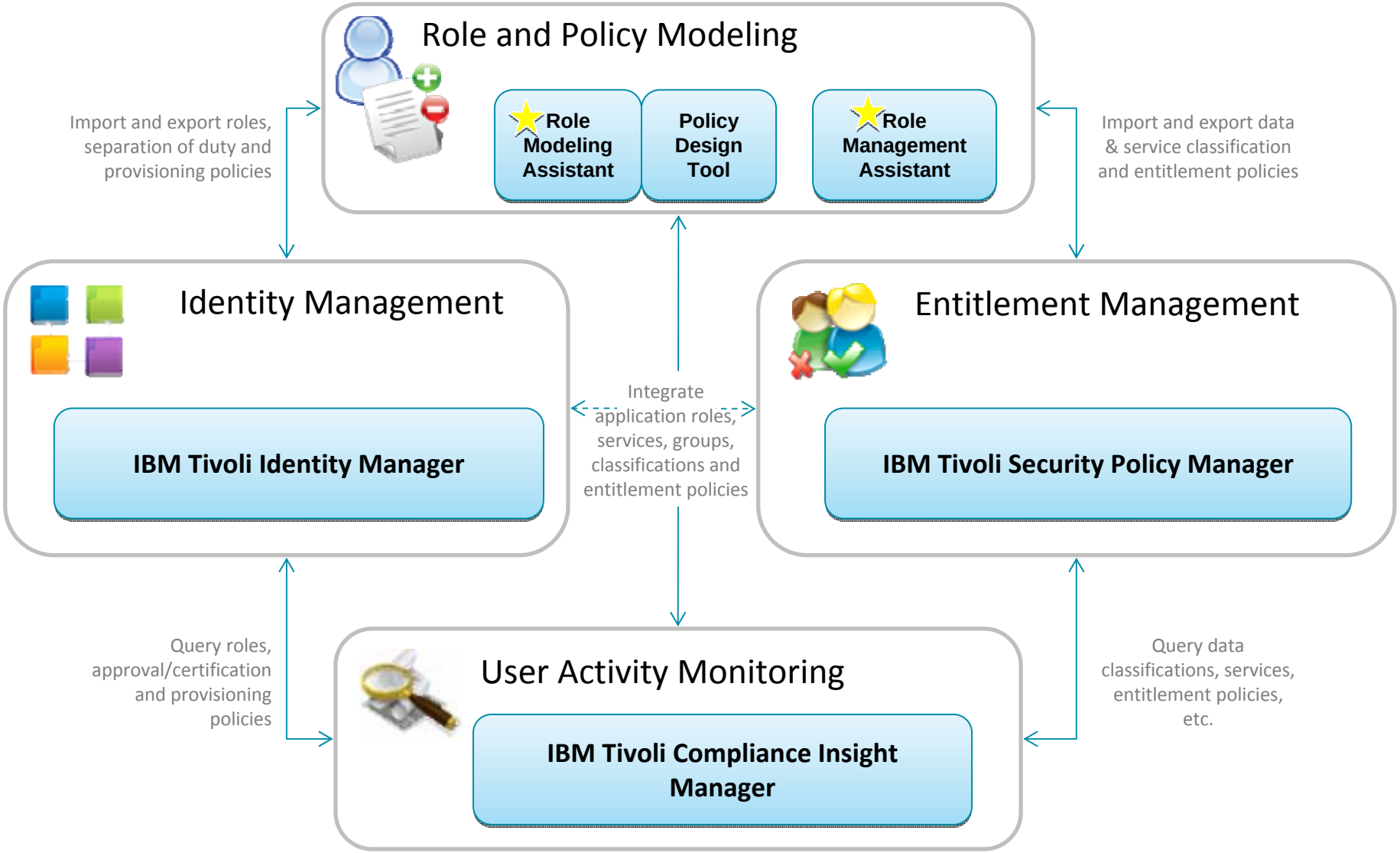
- IBM® DB2®, IBM Rational® Software, IBM Tivoli® Security Solutions, IBM Tivoli Automation Solutions, IBM WebSphere® Software, IBM WebSphere DataPower® SOA Appliance
- IBM System p®, IBM System x®, IBM HTTP Server
- IBM Global Business Services, IBM Global Technology Services, IBM Software Services for WebSphere, IBM Internet Security Services, IBM Research
- IBM Business Partner Saudi Business Machines

IBM's IAM Governance approach



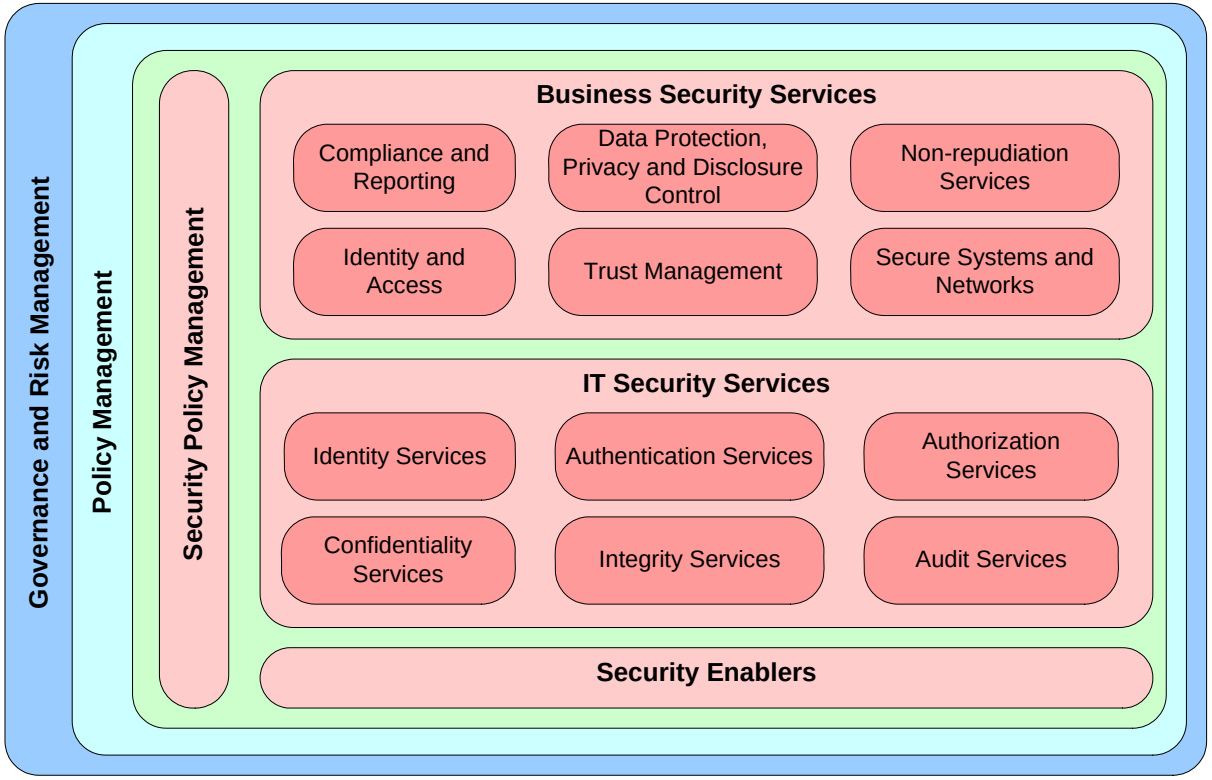
45

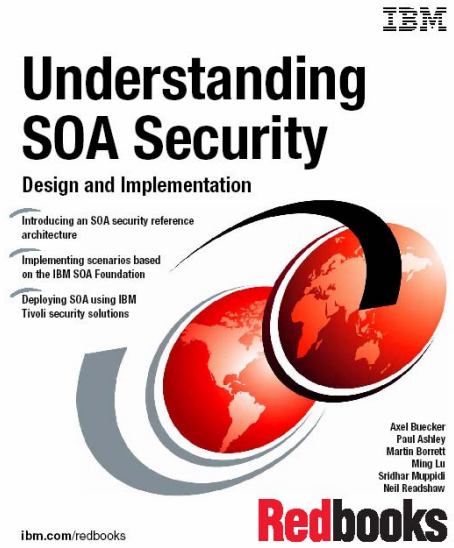
IBM IAM Governance product mapping



46

Current SOA Projects
SOA Security Maturity



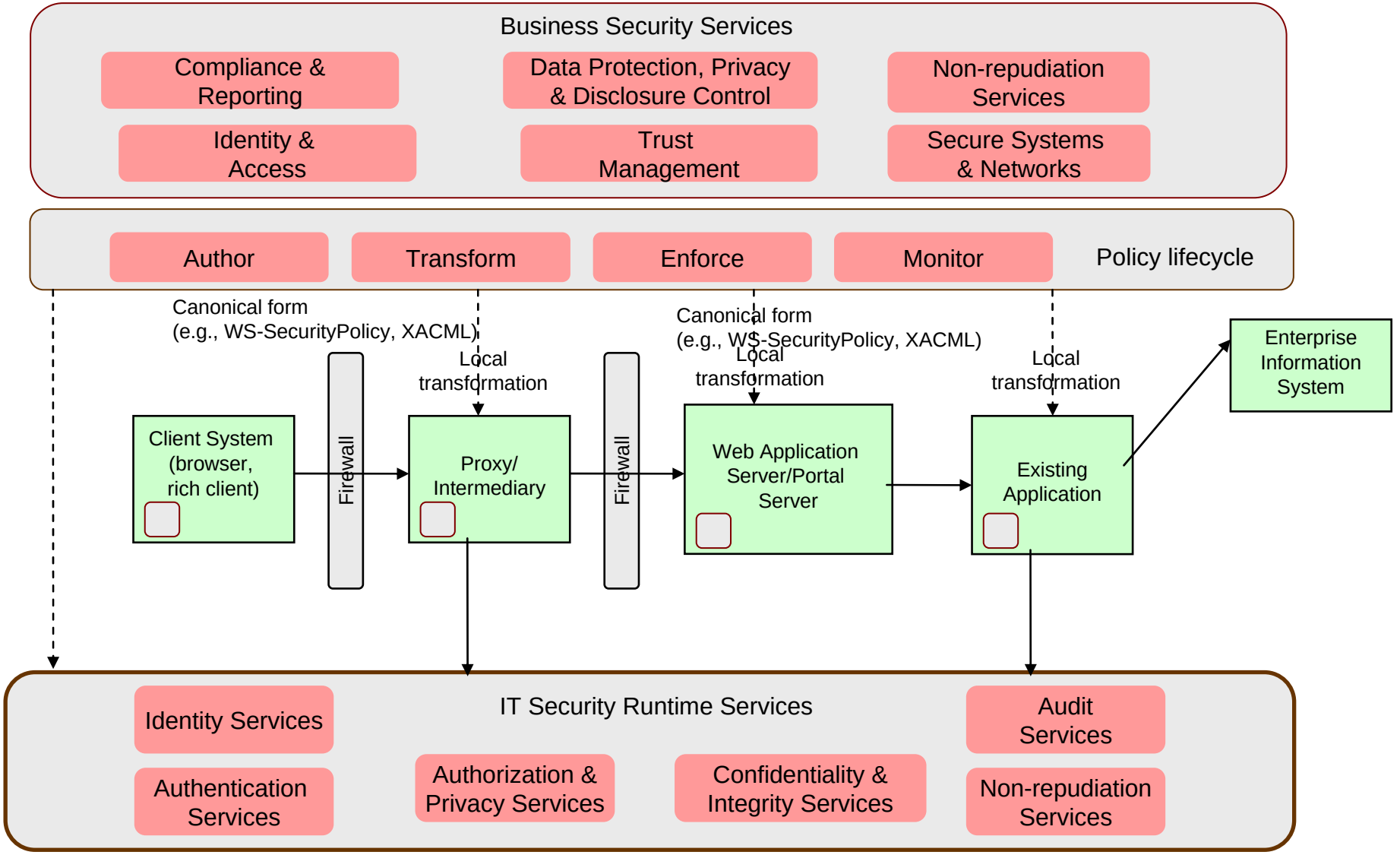


- At various speeds, enterprises are moving to a higher level of SOA maturity
- SOA security is also maturing

Current SOA Projects
SOA Security products

- Very common in SOA projects:
  - Tivoli Access Manager for e-business (TAMeb)
    - Web single sign-on
  - Tivoli Federated Identity Manager (TFIM)
    - Security Token Service for backend integration
  - Tivoli Identity Manager (TIM)
    - Managing the lifecycle of internal users
  - Tivoli Directory Server (TDS)
    - Storing the user identity data
  - WebSphere DataPower XS40 Appliance
    - Providing a web services gateway for connecting to other parties

SOA Security Logical Architecture

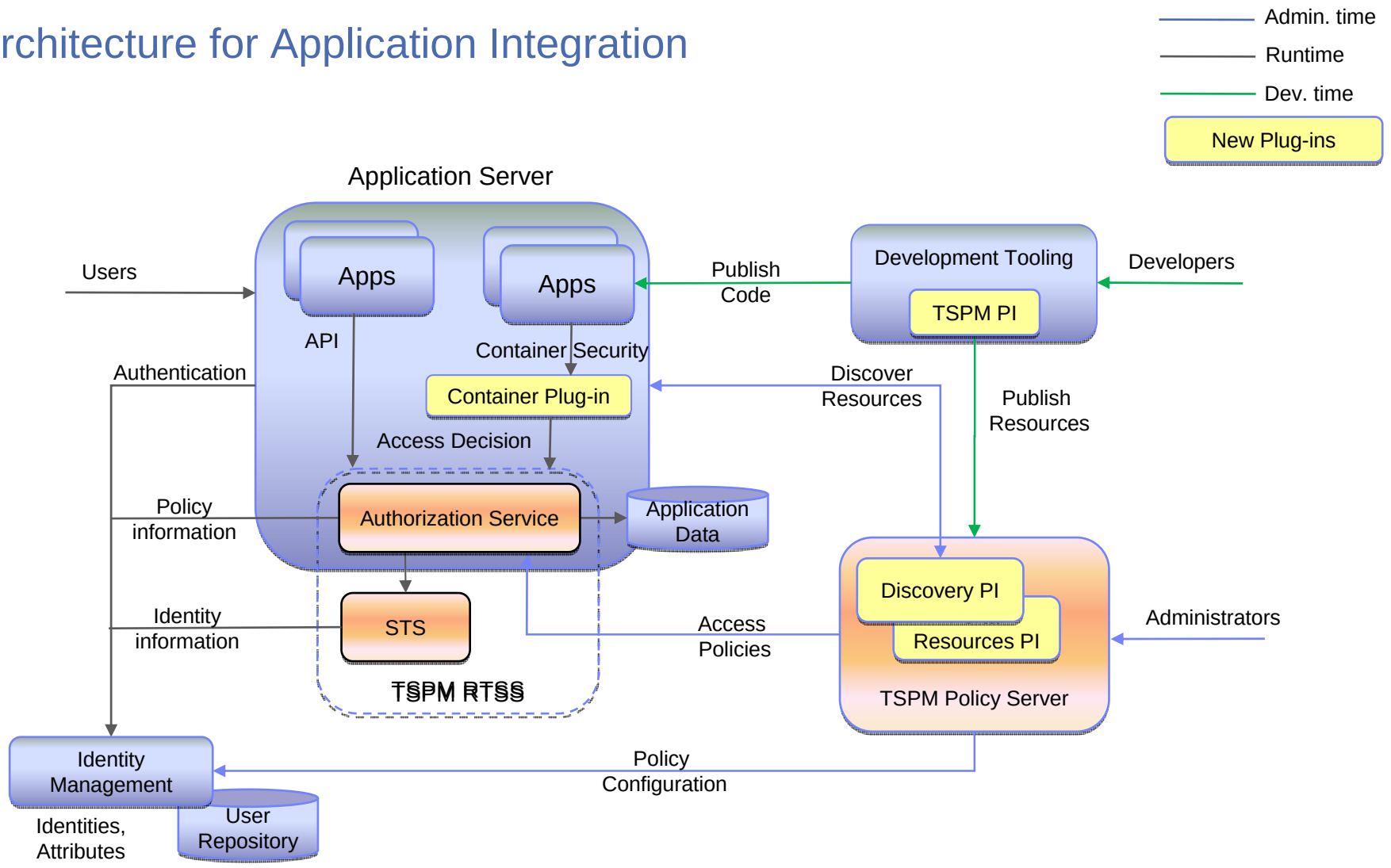


Upcoming Trends – Fine Grained Authorization (FGA)

- **SharePoint Integration**
  - Externalizing Authorization
- **WebSphere Portal Integration**
  - Fine grained authorization within the portlets
- **WebSphere container level integration**
  - Externalizing authorization
- **Session token integration**
  - e.g integration with TAM
- **TSPM management API support for OEM applications**
  - ability to push policies/services to TSPM
  - Support for eWAS

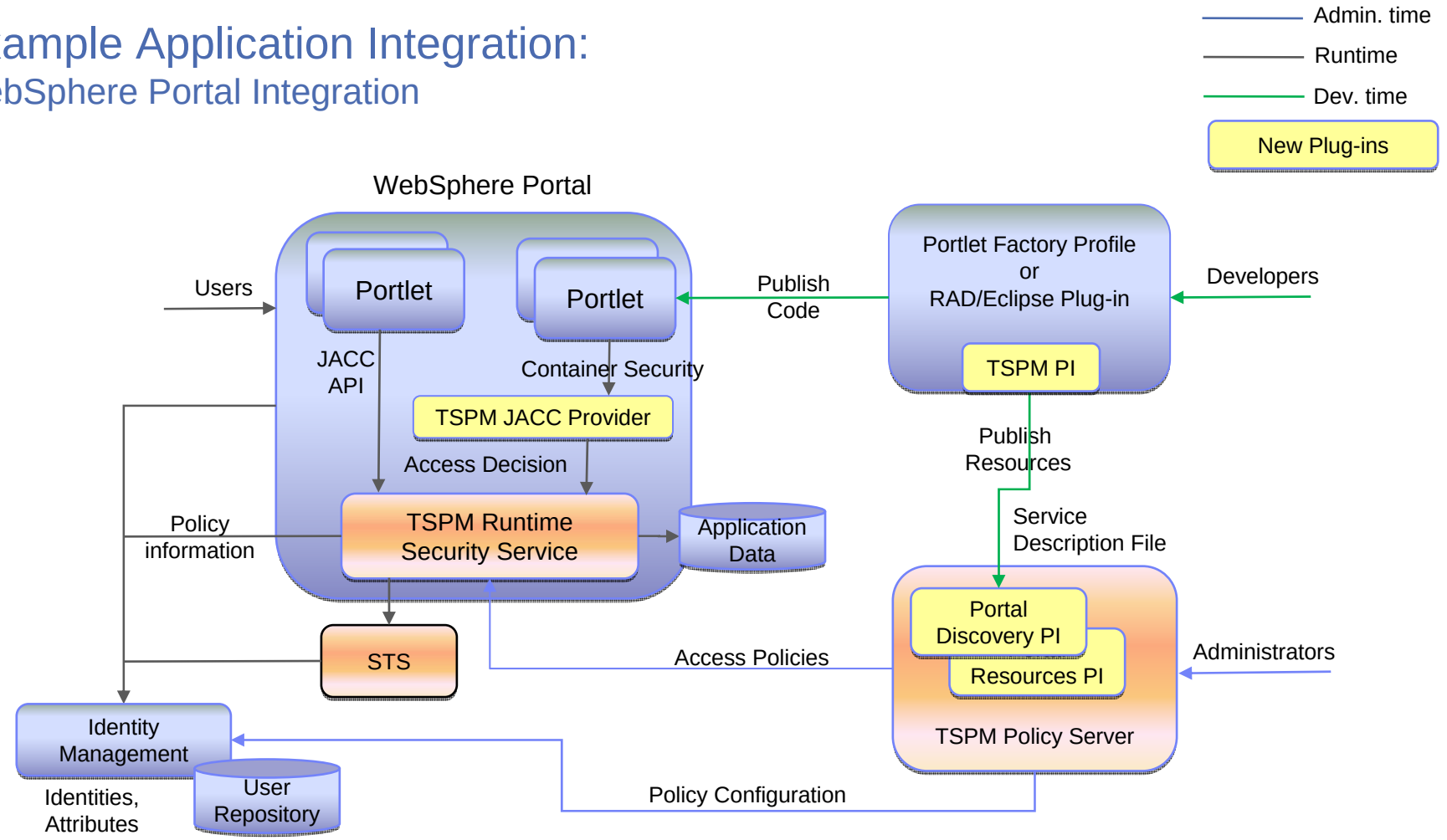
50

Architecture for Application Integration



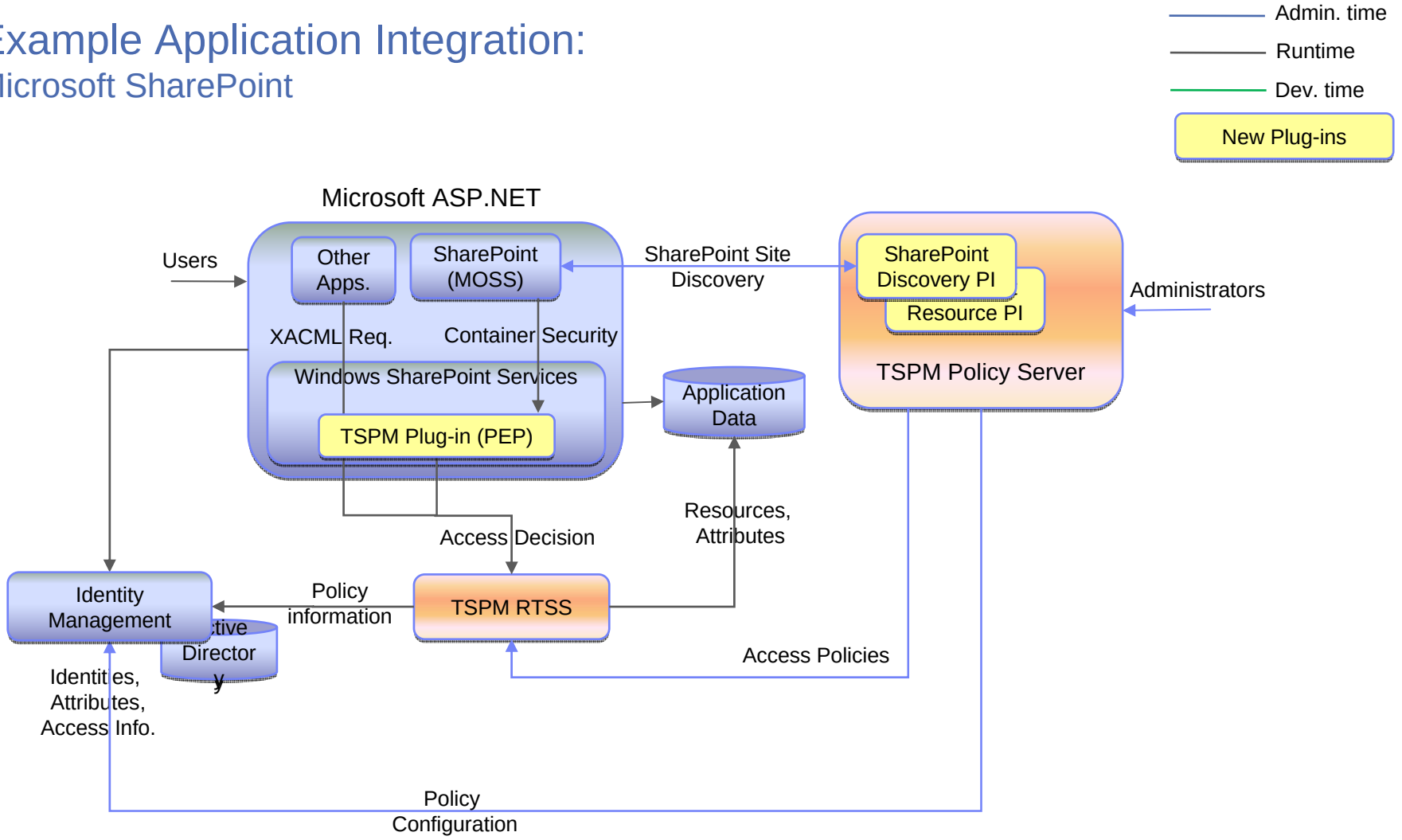
51

Example Application Integration:
WebSphere Portal Integration



52

Example Application Integration:
Microsoft SharePoint



53

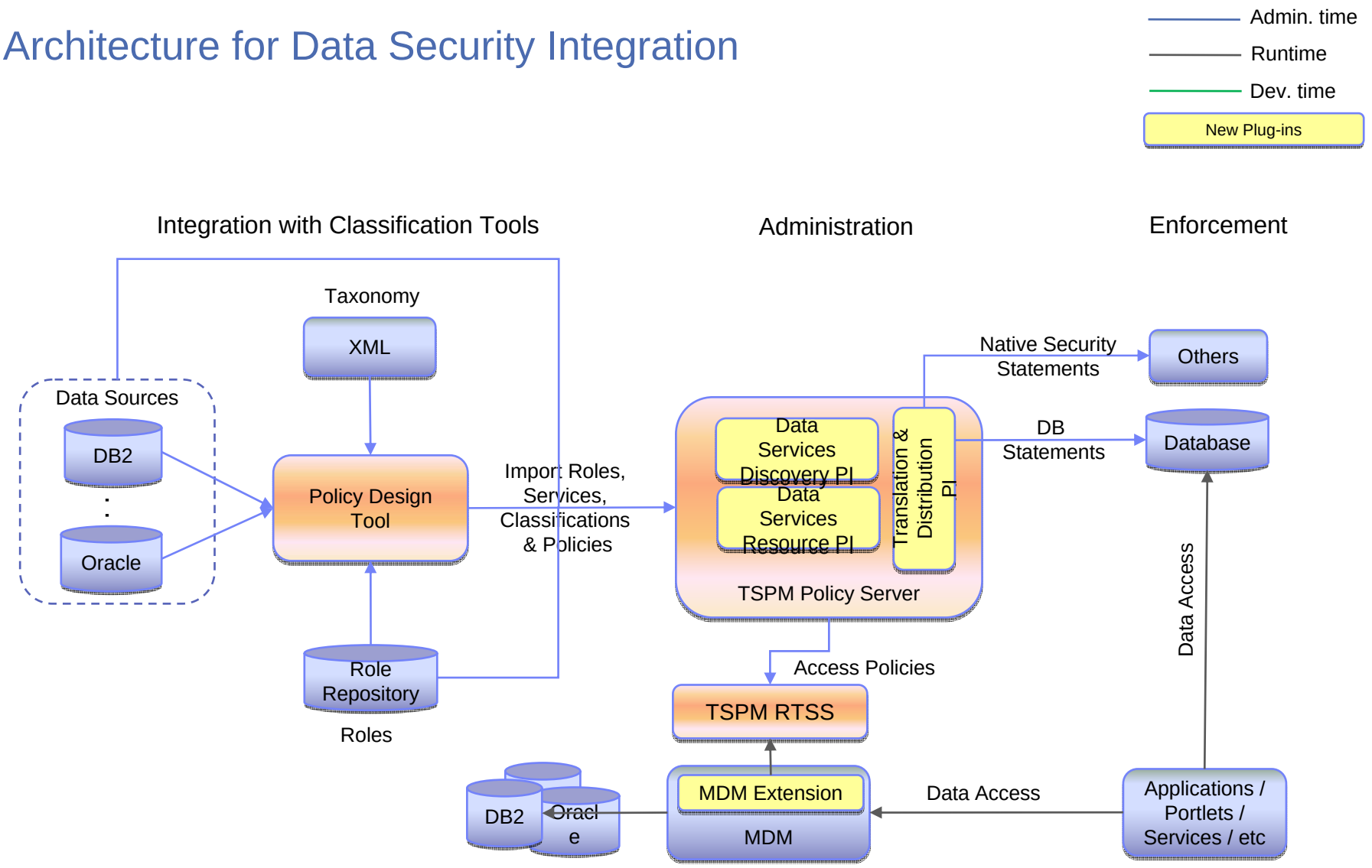
Data Security Theme

- **Integration with Classification Engines**
  - e.g. Policy Design Tool, IBM Classification Module, IIIIS, etc.

- **Integration with Databases**
  - Data level authorization through DB2 GRANT statements and target Oracle Private Database (VPD)

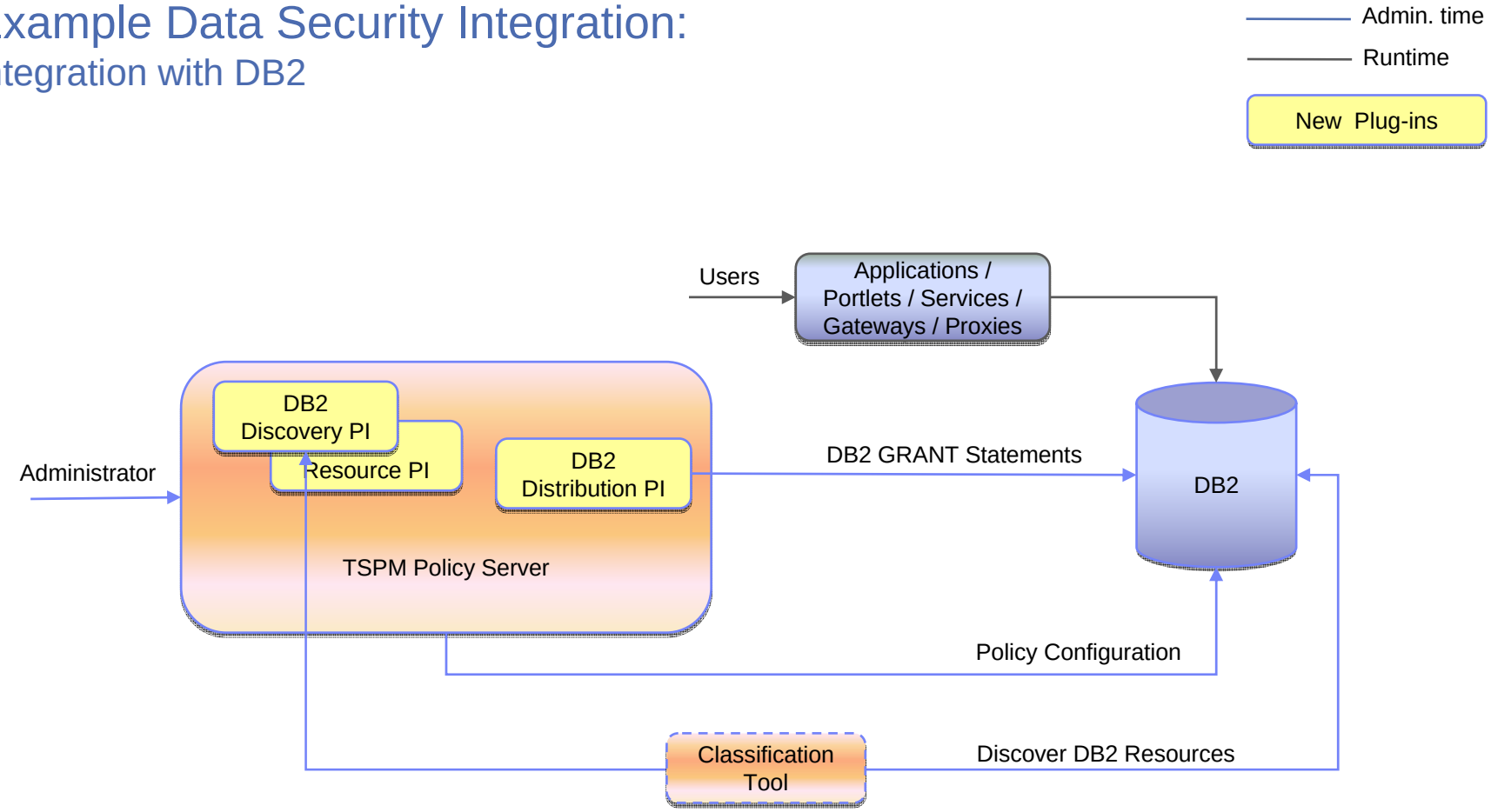
54

Architecture for Data Security Integration



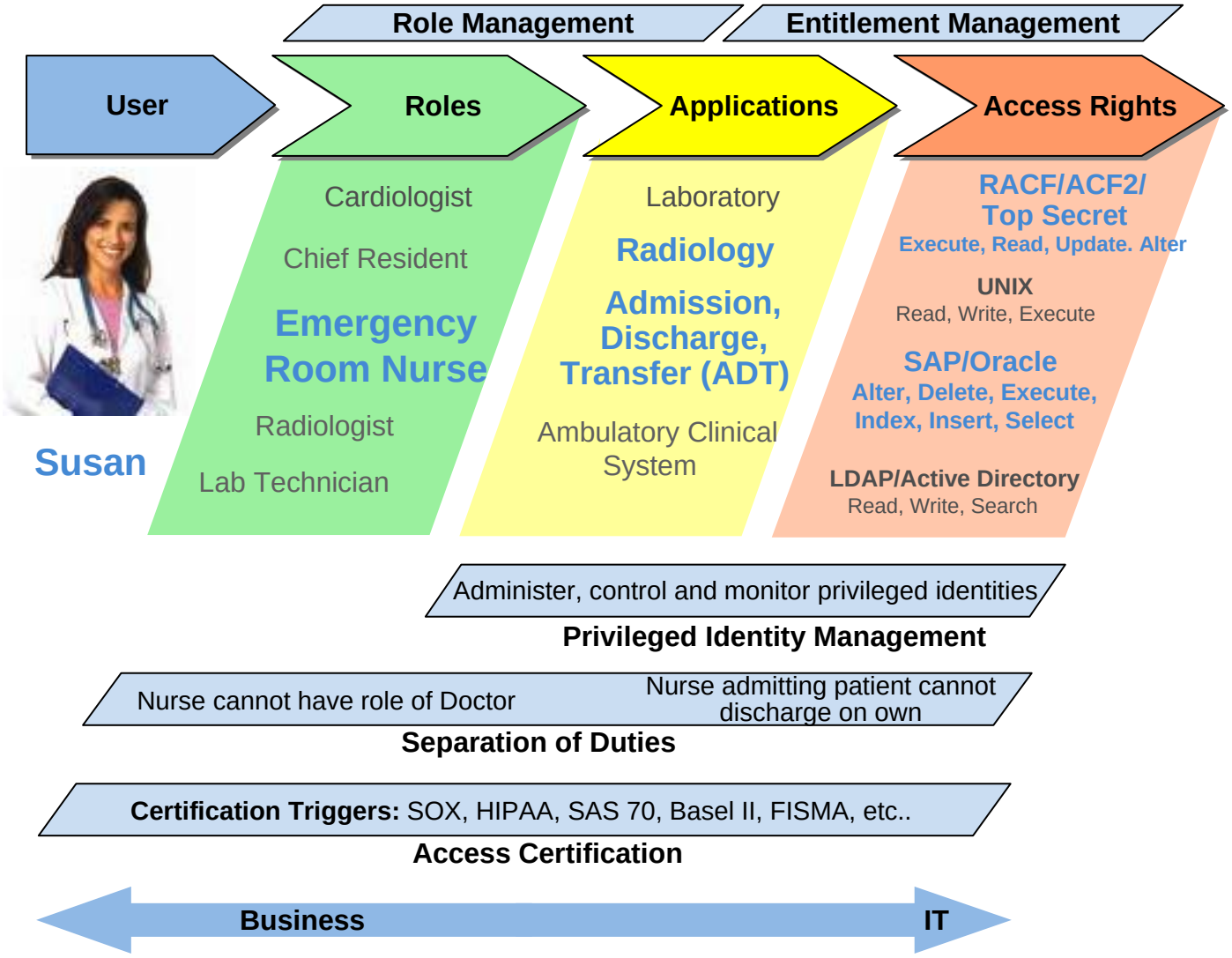
55

Example Data Security Integration:
Integration with DB2



56

IAM Governance delivers a bridge between business and IT



57