Security Integration

Pushing the frontiers of the possible

PulseANZ 2010

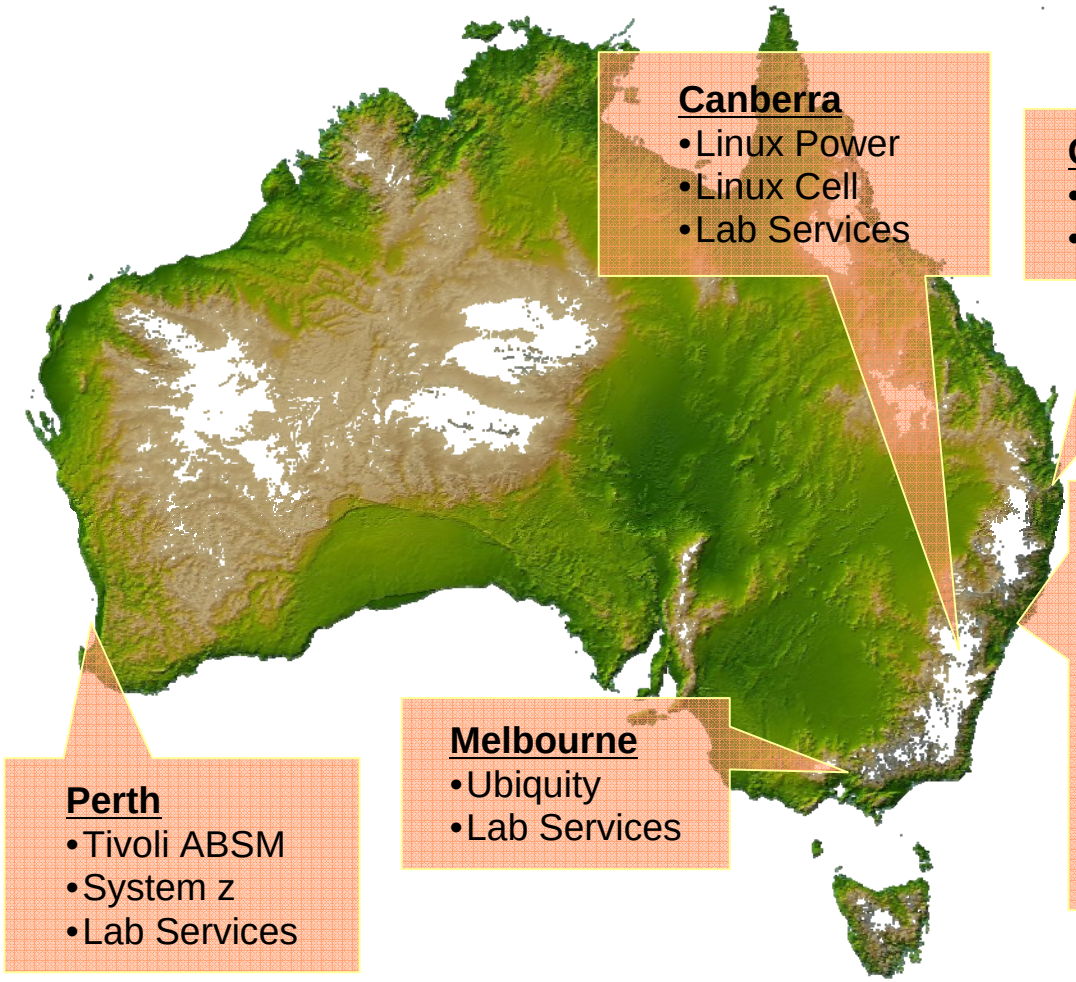
Meet the people who can help advance your infrastructure

Chris Hockings (hockings@au1.ibm.com)

Agenda

- Australia Development Lab Overview
- Looking back at Security Management
- Tivoli Identity and Access Assurance product update
- Authentication storybooks
- Authorization storybooks
- Conclusion

Australia Development Laboratory (ADL)



Canberra
- Linux Power
- Linux Cell
- Lab Services

Gold Coast
- IBM Security Solutions
- Lab Services

Sydney
- WCM, DB2
- Informix, U2
- Ascential
- FileNet, MRO
- Rational
- Tivoli
- Lab Services

Melbourne
- Ubiquity
- Lab Services

Perth
- Tivoli ABSM
- System z
- Lab Services

Australia Development Lab Gold Coast Location

Background

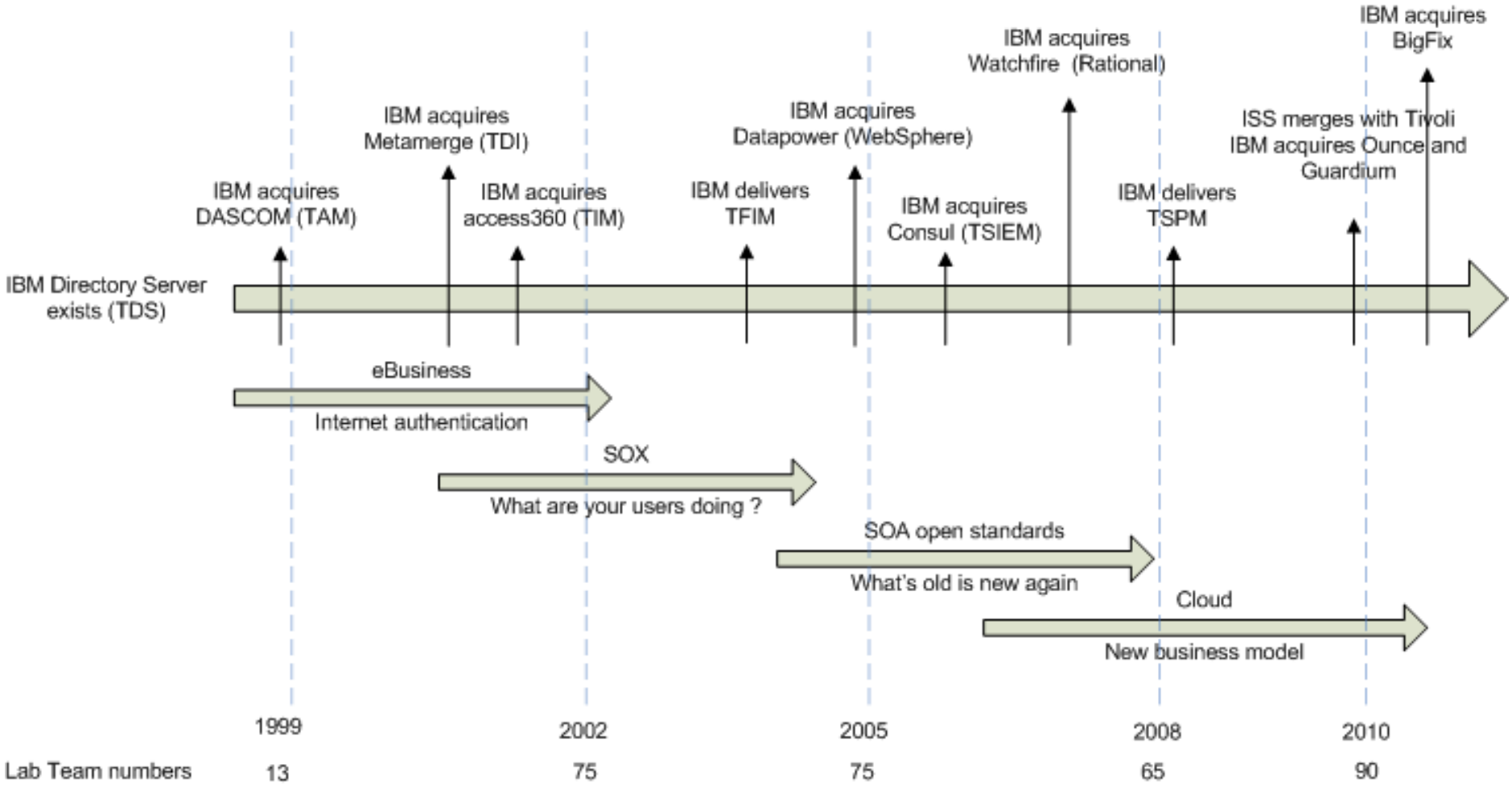
- Founded in 1996
- 1999 acquisition of DASCOM
- Strong links to Queensland universities
- 90 technical staff
- Covering entire software lifecycle
- Design, dev, test, service support

Missions

- Tivoli Access Assurance development
  - Tivoli Federated Identity Manager
  - Tivoli Security Policy Manager
  - Tivoli Identity Manager
  - Tivoli Integration Factory
- ISS product development
- **Solutions group (Support, Services)**

Built on client trust, innovation, dedication to <u>your</u> success

A brief look through Identity Management history

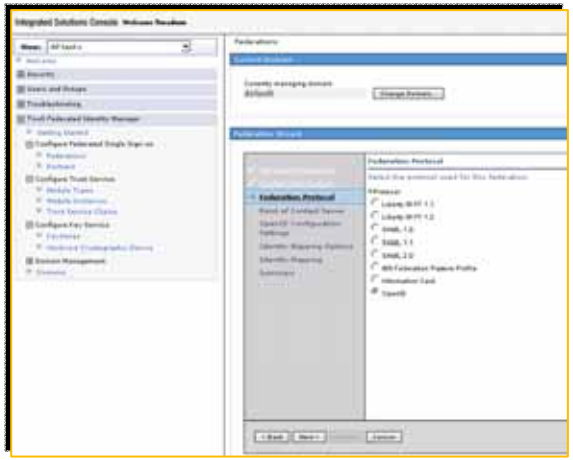


Recent Identity product updates

IBM Tivoli Access Manager for e-Business (TAM)
IBM Tivoli Federated Identity Manager (TFIM)

New Features / Capabilities

- Performance improvements
  - New Java admin API to manage large scale deployments
- B2C user self service
  - User enrollment, validation for seamless authentication & password change/reset with secret questions



- Ease of admin / deployment support
  - Clustering support and ease of replication for TAMeb WebSEAL
  - Flexible health check for TAMeB application's status
  - Standards-based junction support for application integration
    (e.g. SAML, Kerberos, RACF Passticket junctions)
  - Serviceability improvements, session cache, ITDS password policy, cookie jar, tracing etc.
- More out-of-box integration
  - Updated SSO integration for key 3rd party applications
    (e.g. SharePoint, .NET, WAS, SAP, Oracle)
  - SAML 2.0 (attribute query, protocol interoperability)
  - OpenID (attribute support)
- Identity service to validate on- and off-premise access including cloud/SaaS deployments
  - Supports Lotus Live, Google Apps, Salesforce.com, Webex

IBM Tivoli Security Policy Manager (TSPM)

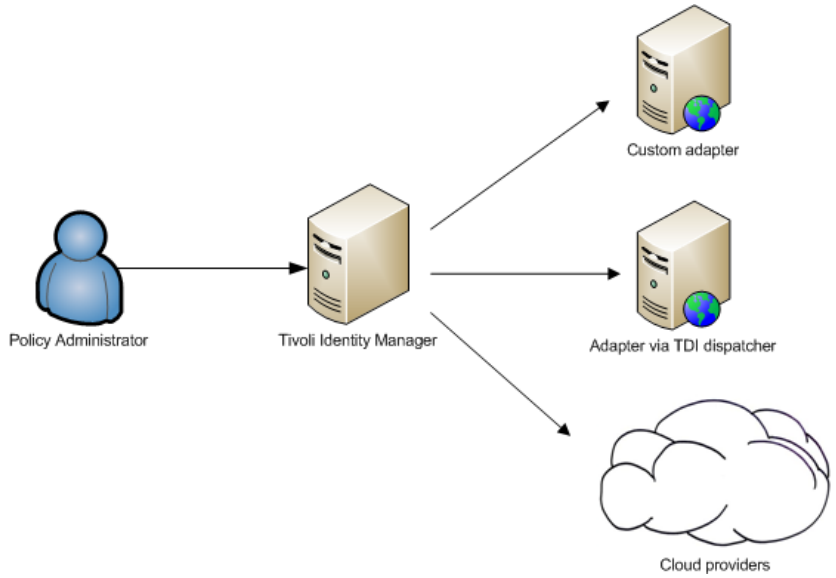
- Open standards security policy languages have provided interoperability and flexibility for authorization (entitlements) policy management

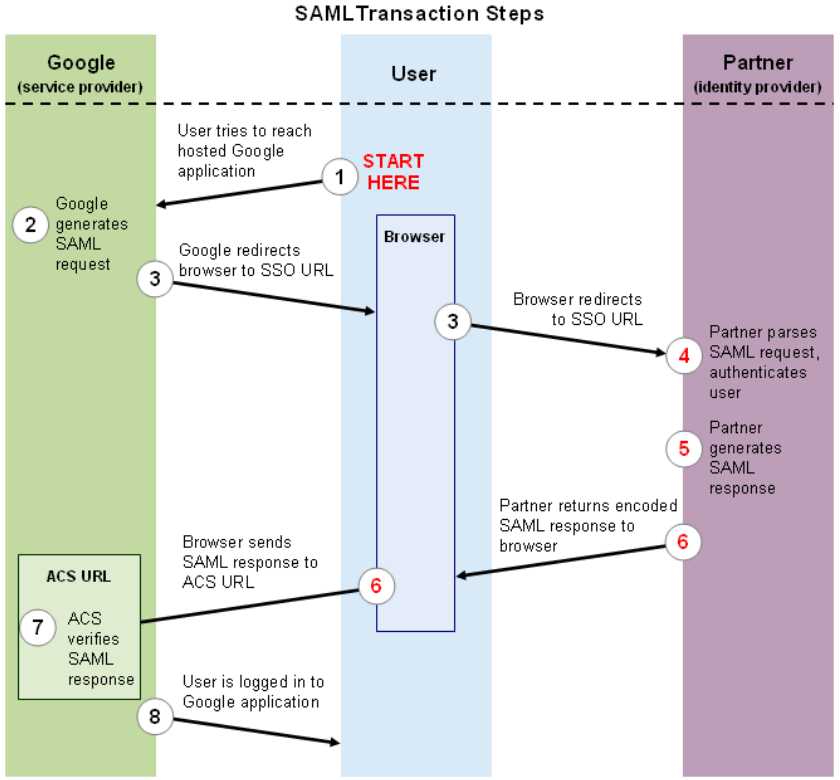
- Message protection policy for SOA environments
  - Relevant standard is WS-SecurityPolicy
  - Integrated with typical web service repositories, such as WSRR
  - What token type is required part of the Web Services request ?
- Entitlements management for applications and data
  - Relevant standard is XACML
  - What are the user's entitlements ?
  - Is the user authorized to perform an operation on a resource ?
- Out-of-the-box integration for data entitlements enforcements
  - Applications (e.g. WebSphere Portal, WAS, .NET Sharepoint)
  - Content managers (e.g. SharePoint, FileNet)
  - Databases (e.g. DB2, Oracle)

Authentication storybooks

Google cloud integration using TFIM and TIM

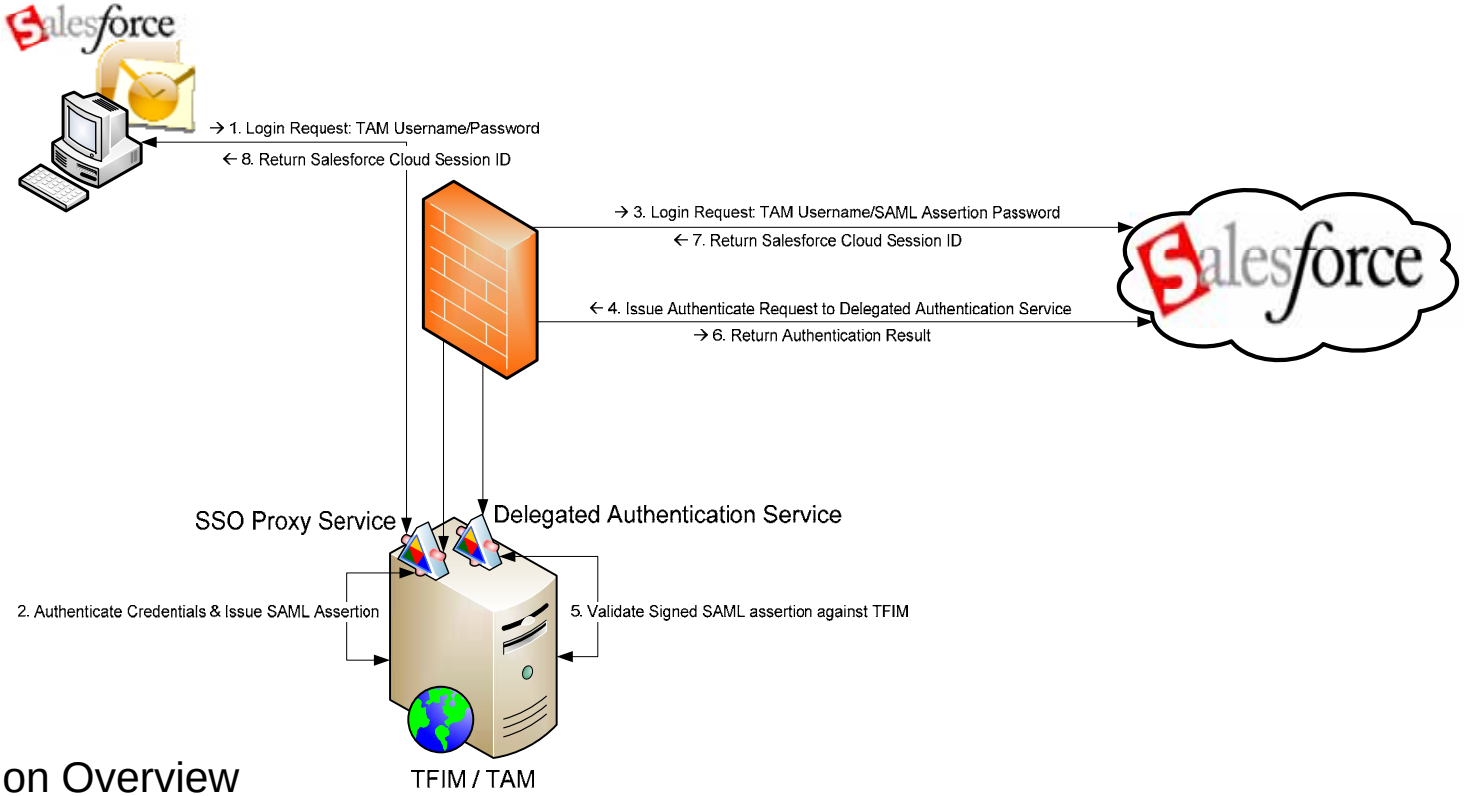
- SAML SSO scenario with Google Applications
  - https://www-950.ibm.com/blogs/sweeden/?lang=en_us
- Standards work needs to settle for identity provisioning into the cloud
  - SPML future is still uncertain, SAML and OAuth still evolving
- Identity provisioning into the Google cloud is being demanded by customers





SalesForce.com cloud integration using TFIM

- Users have one internal password and this password needs protection
- Salesforce.com cloud provides integration specifications for security service



- Solution Overview
  - Custom developed Web Service Proxy
  - TFIM trust service for TAMeb password authentication and SAML token generation
  - Custom authentication service for SAML token validation

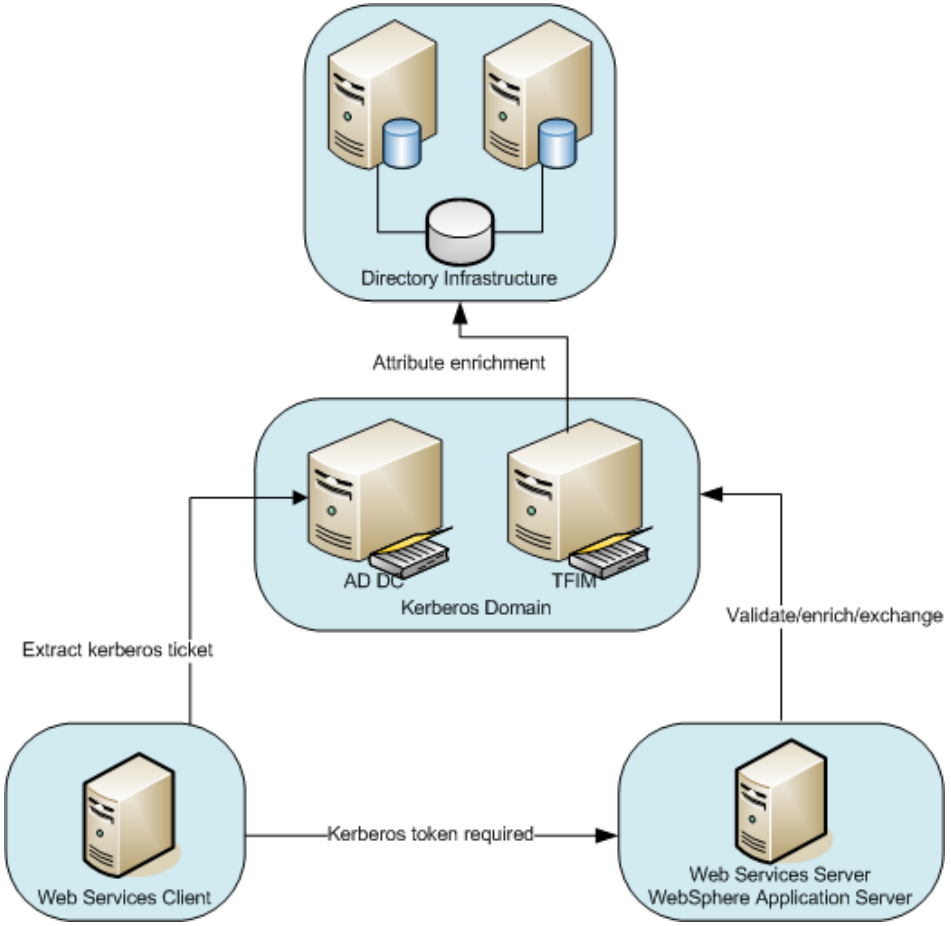
"My data on someone else' disk" –Bruce Schneier, RSA conference 2010

Identity propagation using TFIM

- Demonstrating TFIM Kerberos to SAML token exchange in a Windows environment

- Customer's requirements:
  - Demonstrate token exchange
  - Kerberos to SAML conversion
  - Attribute enrichment mandatory
  - Ability to create a WAS subject

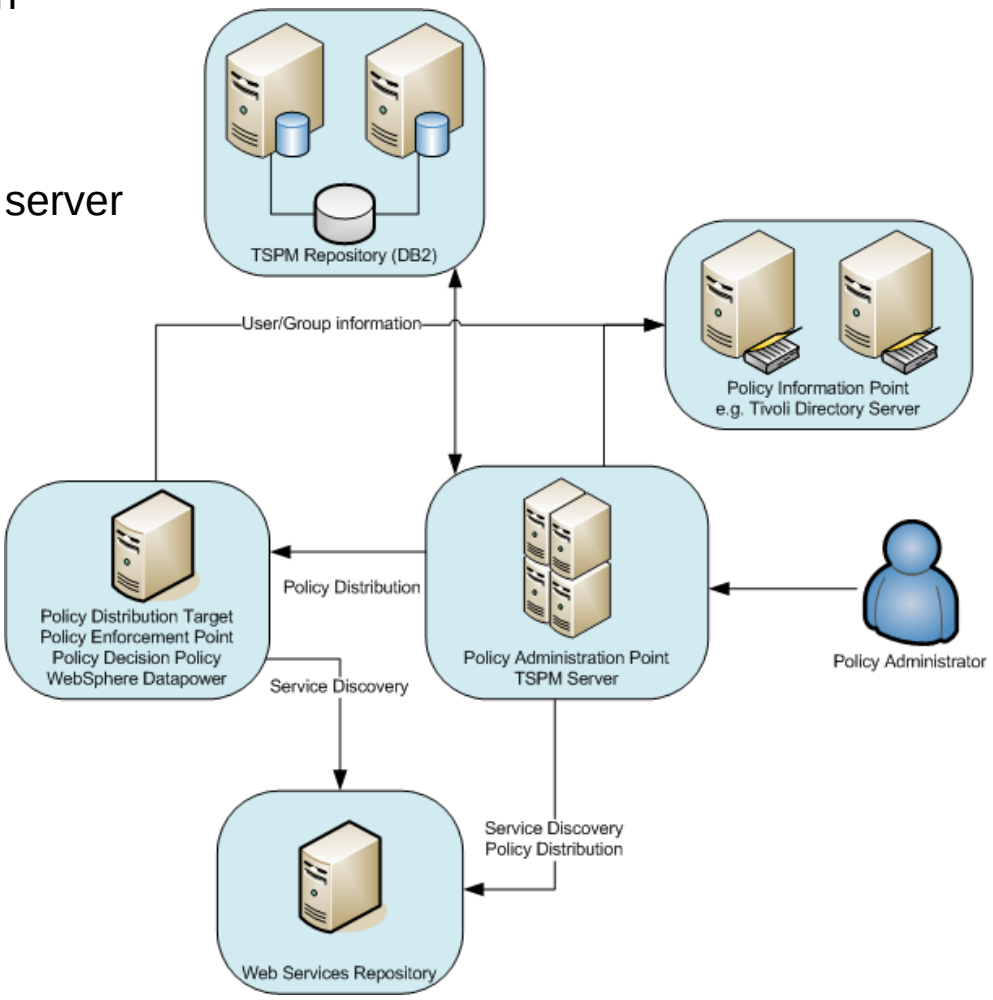
- Solution Overview
  - TFIM acting as the Trust Service
  - TDI attribute enrichment
  - Programmatic enrichment
  - Custom Web Service
    - Based on EchoApplication



Authorization storybooks

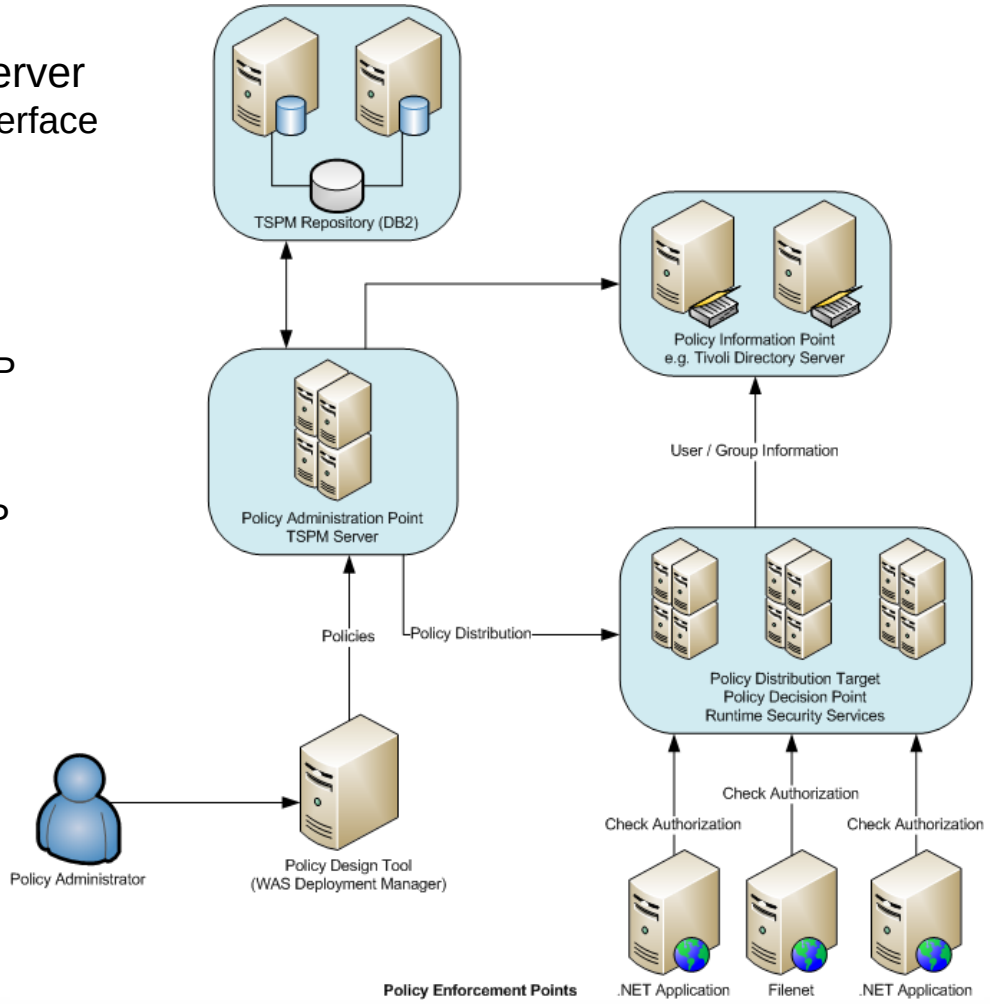
SOA security patterns using IBM Security Solutions

- Standard TSPM for SOA deployment pattern
- Service discovery to WSRR
- Message protection policy applied at TSPM server
- XACML policy applied at TSPM server
- Modified service returned to WSRR
- TSPM pushes XACML policy to Datapower
- User information can be pulled from PIP



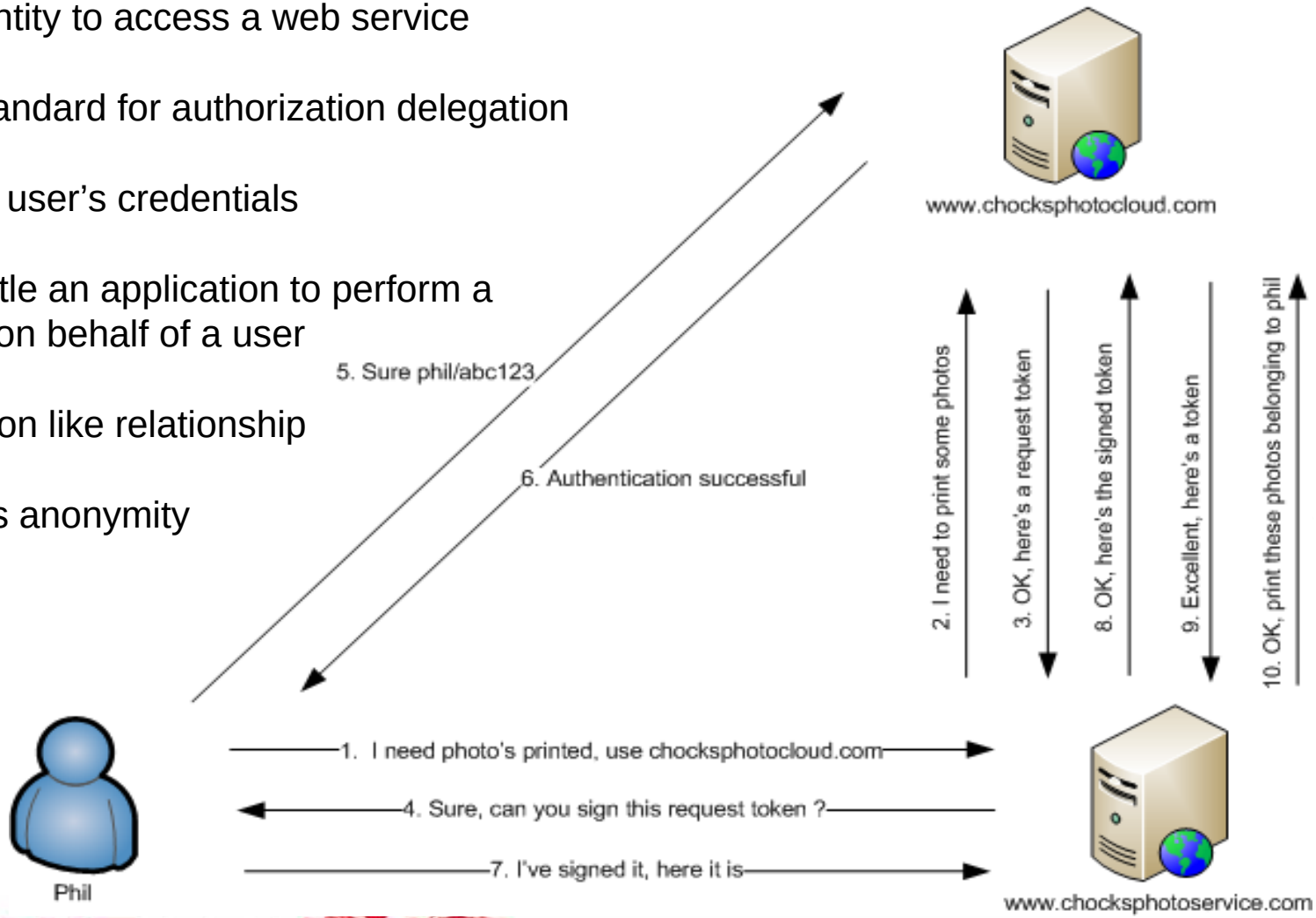
Fine grained programmatic authorization

- Standard TSPM for Entitlements deployment pattern
- Service discovery custom or application server
  - SharePoint integration uses a standard interface
- XACML policy is defined and distributed
- Local mode enforcement
  - Requires application being a PDP and PEP
- Remote mode enforcement
  - Runtime Security Services (RTSS) as PDP
  - Application is the PEP
- Data level integration
  - Available for DB2 in TSPM 7.1
  - Oracle and Filenet being considered



OAuth delivers delegated authorization capabilities

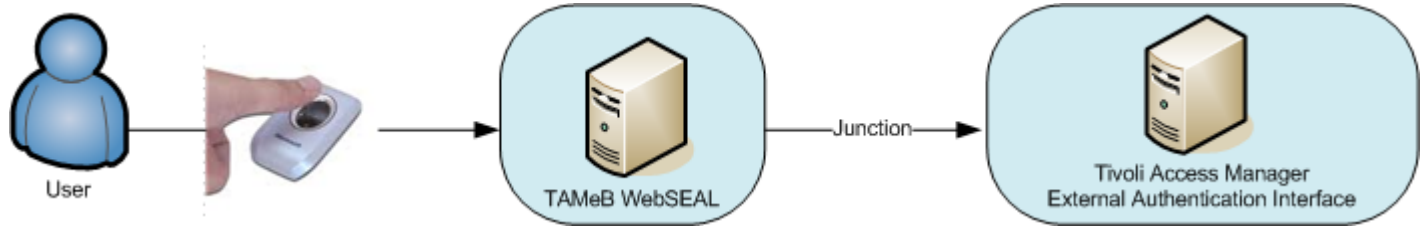
- A method that allows an end user to delegate authorization to a web application to use their identity to access a web service
- Open standard for authorization delegation
- Protects user's credentials
- Can entitle an application to perform a request on behalf of a user
- Federation like relationship
- Supports anonymity



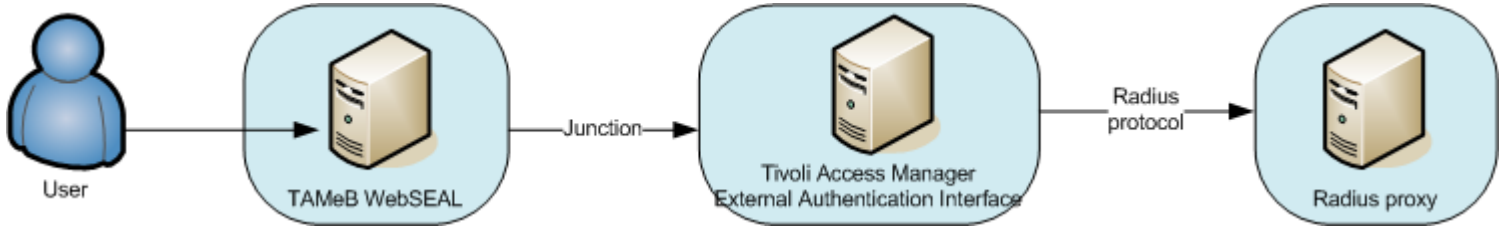
Others

Other authentication customizations

- TAMeB WebSEAL authentication solutions delivered include:
  - Picture based authentication, i.e. remember 3 pictures, in order, for authentication
  - Fingerprint authentication

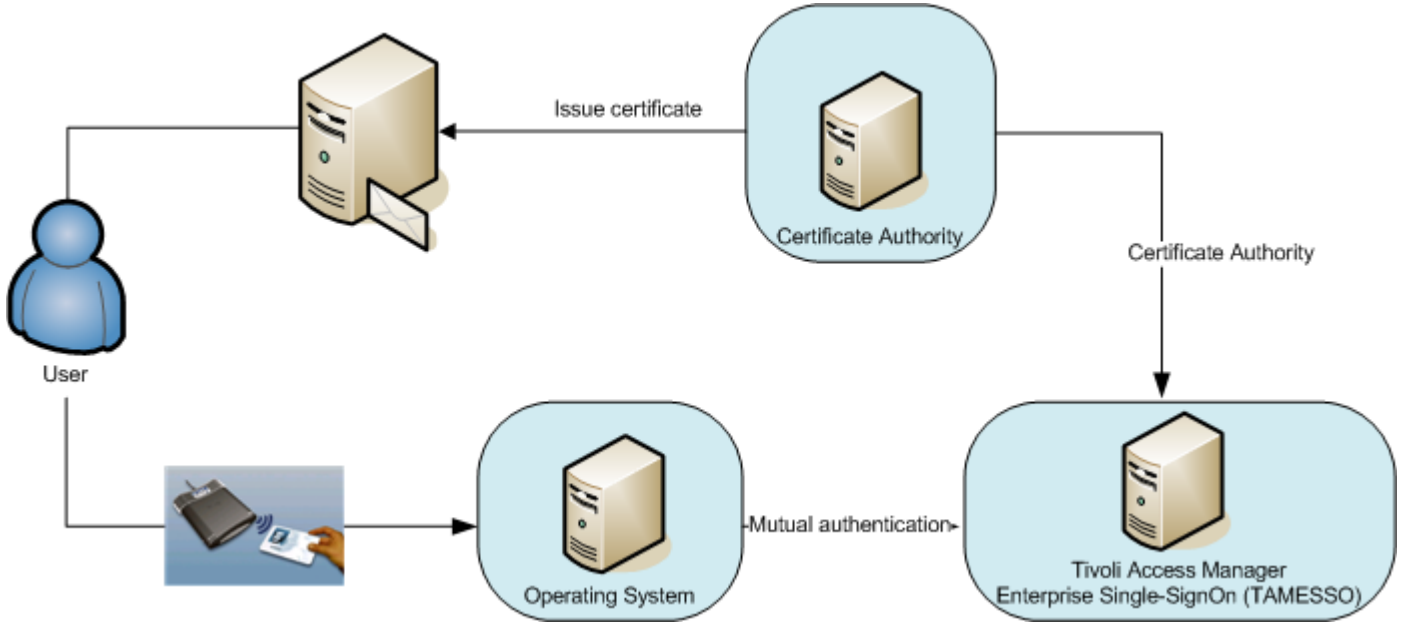


  - Radius authentication



Enabling citizen centric authentication

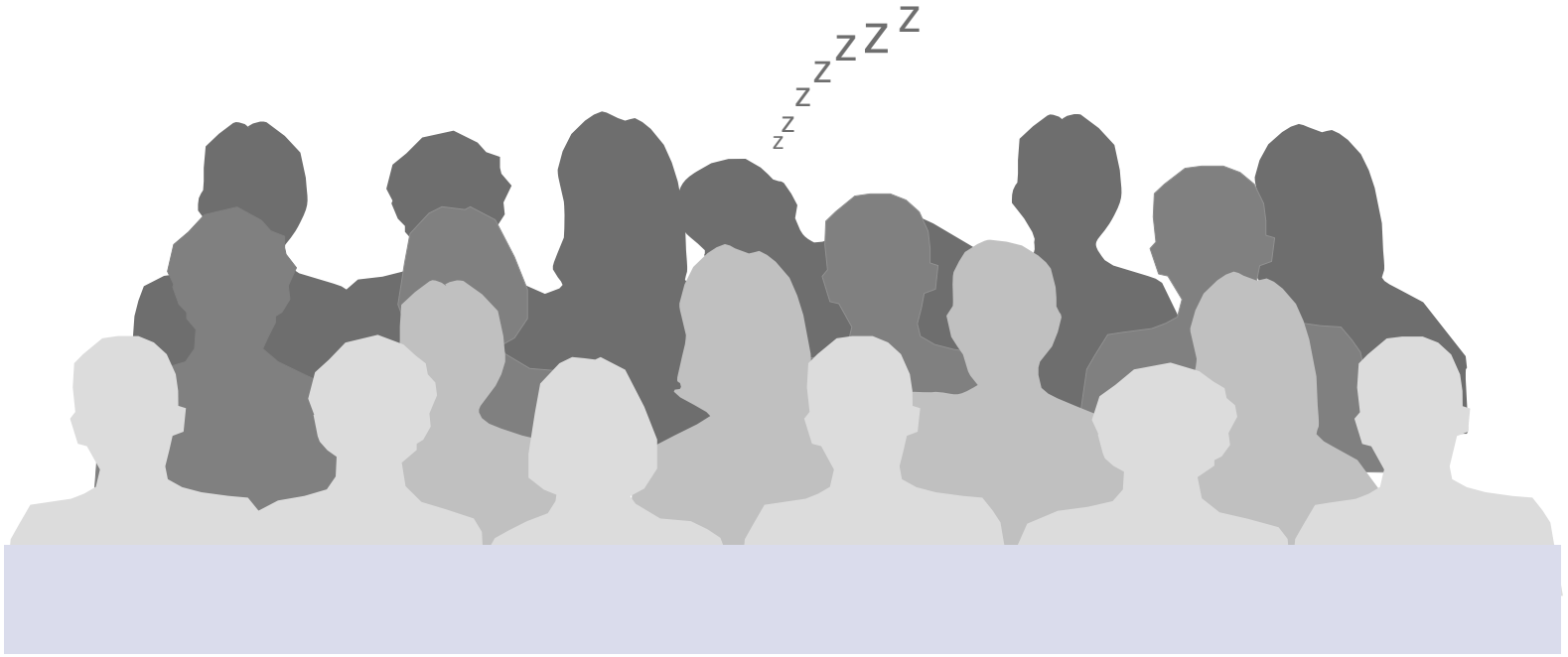
- TAM E-SSO provides support for strong authentication using certificates
- This support breaks down when the PKCS#11 library is not supported within TAME-SSO
- ADL Gold Coast developed and delivered a generic cryptographic service provider (CSP) capable of supporting government based Certificate Authorities within TAME-SSO
  - A Generic CSP is able to configure in support for any PKCS#11 certificate



Looking forward from here

- Within Tivoli Security, Identity and Intrusion are singing from the same hymn book
  - Merging of Tivoli and ISS has created a new synergy
  - Many strategic roadmap initiatives in Tivoli's development pipeline
- The creation of the IBM Security brand has encouraged strategy alignment across all pillars
  - Hardware, Software (WebSphere, Rational, Tivoli and Information), Services
  - Appliance strategy is starting to evolve
- ADL Gold Coast continues to lead in delivering worldwide products and customer satisfaction across a broader mission
  - 2010 expansion has resulted in 5-6 new product development missions
  - Great for our local Australian and Asia customers
  - Your continued help in driving product evolution is invaluable
- We would like to hear from you, and your experiences with the Identity products

Come to the IBM Security Booth



Trademarks and disclaimers