

Identity & Access Management (IAM) Reference Architecture

How the different Areas in IAM fit together

A comprehensive approach to an IAM reference architecture and its delivery approach.

More Information

PDBS Website:

<http://www.pdbsec.com/>

SAML & SPML standards:

<http://www.oasis-open.org/>

Liberty Alliance project:

<http://www.project-liberty.org/>

Vendors of Note:

[Computer Associates](#)

[IBM](#)

[Oracle](#)

[Sun](#)

[RSA](#)

[Novell](#)

[PassLogix](#)

[PingID](#)

[PSynch](#)

Pacific Data Bank Security

Contact

Name: Neil Rerup

+1 604 948 9326

nrerup@pdbsec.com

Introduction

In order to meet the business challenge surrounding IAM, this paper provides an overview of an Identity and Access Management (IAM) reference architecture and its delivery approach.

Executive Overview

Identity & Access Management deals with two areas; Access Management and Identity Management. Access Management is involved when trading partners, customers or employees of an enterprise require or are allowed access to the infrastructure and data held within. Identity management goes beyond simple password management or synchronization and manages the profiles of the individuals or systems used within the Enterprise.

Drivers

Due to the increasing importance of IAM, the compelling reasons for enterprises to adopt IAM technologies can be summarized by the following drivers:

- Automate manual business processes and improving the ROI of the IT Infrastructure.
- Put proper policies and controls in place for managing user access across all business platforms and resources
- Provide proof of controls through monitoring and auditing capabilities to internal and external auditors to meet regulatory compliance
- Improve business performance by securing and better enabling access to applications
- Improve both external and internal user's productivity and efficiency while reducing Help Desk and system administration cost
- Meet the growth of business ecosystem by simplifying the management of the users and their accesses
- Securely expand business online with customers, vendors, partners and suppliers.
- Integrate IAM processes into the entire IT Service Management strategy to better align IT with business objectives

Delivery Approach

There are four primary components in Identity & Access Management. Which component you start with is dependent on the priorities of the organization but the logical flow of developing a complete IAM Architecture flows in the manner of the following Diagram.

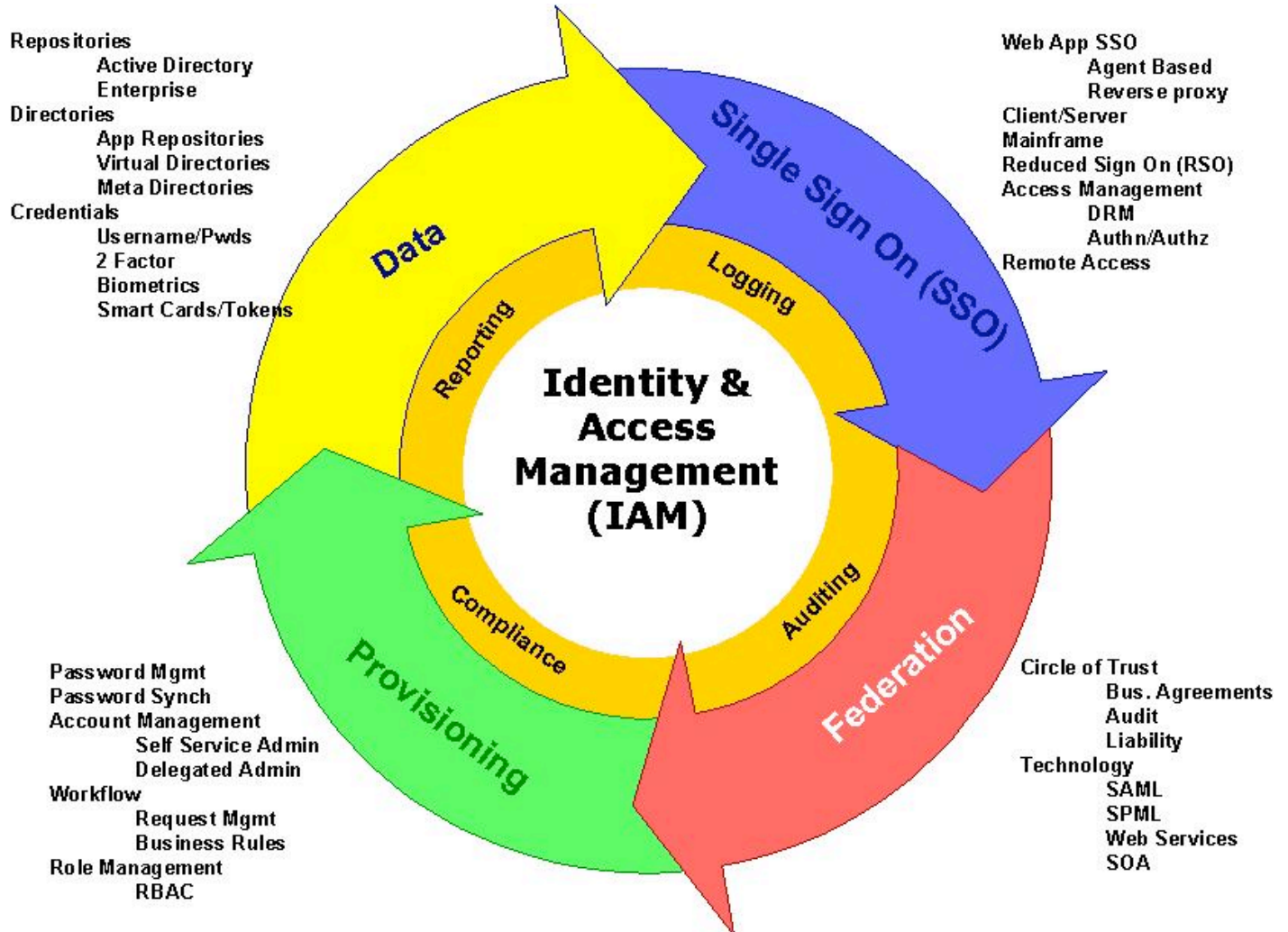
- Data – management of the Enterprise's Repositories and information held within
- SSO – Access Management to Enterprise Resources, regardless of the number of credentials presented
- Federation – Extending Access Management to the domain's of business partners in order to make business processes as seamless as possible
- Provisioning – Managing Identity Information in an effective manner. Extends into Workflow activities.

Each component is dependent on the one previous. For example, Provisioning affects the data repositories so that Identity information is consistent. The data in the SSO Policy stores and repositories affect the SSO solution. Federation extends SSO to multi-domains. Identity and Access Management is an integrated eco-system that has a logical development process.

IAM Reference Architecture in Detail

Introduction

Managing the user identities and access rights of the enterprise has become a primary concern for IT organizations today. The interest in Identity and Access Management (IAM) is driven by the combination of increasing regulatory compliance requirements and the ongoing need for IT to reduce costs and manage risk, while improving business performance at the same time.



Solution

The PDDBS IAM reference architecture and delivery approach provide broad coverage across applications and platforms including legacy, distributed and web environments, covering 4 major elements of IAM as well as a 5th common element related to Audit. Each of these 5 major elements is dependent on each other and there is a logical flow to the implementation of each of these elements. The 5 Elements are:

1) Data:

Data deals with the management of data repositories within the Enterprise. These repositories contain all the information associated with Identity and Access Management (eg. Identity information, access privileges, IAM Policies, etc.). Typically, the Data Element is associated with:

- **Repositories**
 - **Active Directory** – typically used for Domain logon

- **Enterprise Repository** – for use in storing Enterprise standard information accessed by multiple resources
- **Repositories**
 - **Application Repositories** – storage of Application specific authorization information
 - **Virtual Directories** – creation of virtual repositories within single physical instances of directories
 - **Meta Directories** – repositories of Meta information.
- **Credentials**
 - **Username/Passwords** – the most common form of authentication information stored
 - **2 Factor Authentication** – Often, Enterprises require higher levels of authentication to access more sensitive information. This type of information is typically:
 - **Biometrics** – Biometrics allows an Enterprise to assign an account parameter to an individual's physical characteristics
 - **Smart Cards/Tokens** – Smart Tokens/Cards are devices that are used to supplement Username & Password by adding a 3rd parameter: Something a Person Has.

2) Single Sign-on (SSO):

SSO provides full-featured access to resources across the extended enterprise. This IAM Element contains

- **Web Application SSO**
 - **Agent based** – use of agents located directly on the Application Servers
 - **Reverse Proxy based** – use of a Reverse Proxy for Applications more difficult to integrate with as well as used in a more centralized approach.
- **Client/Server** – often referred to as Enterprise SSO (ESSO), this involved placing Access Management clients on the desktop to automate the logon to Client/Server applications.
- **Mainframe** – Access Management to Mainframes typically call for a XML shell to integrate SSO solutions with 3270 Terminal Emulation;
- **Reduced Sign On (RSO)** – the ideal goal for an Enterprise is true SSO, where the user only has to sign in once during the day. The more typical, cost effective solution is usually reducing the number of sign on instances to as few as possible;
- **Access Management** – Access Management involves the actual access to file level information. This can come in two forms:
 - **Digital Rights Management (DRM)** – DRM is a system that allows the access information to follow the file, regardless of where the file is moved to
 - **Global User IDs (GUIDs)** – GUIDs are IDs that are unique to an individual and contain information about the individual based on the construction of the GUID ;
- **Remote Access** – There are actually two locations that a User can be when trying to access an Enterprise's resources, Internally or Externally. So when a User tries to access Remotely, the VPN or Citrix solution needs to be considered in the SSO solution.

3) Federation:

Identity federation provides an enhanced user experience, competitive differentiation, reduced costs and improved security and ensure secure access from or to applications of customers, vendors, partners and suppliers. It includes:

- **Circle of Trusts** – Circles of Trust are the business arrangements set up for allowing the passing of authentication information from one Enterprise to another. These business arrangements are MORE important than the technical aspects and typically consist of:

- **Business Agreements** – Without the business agreement detailing how levels of assurance are obtained between partners, the partners will not know how much they can trust any authentication provided to them through a Federation solution
 - **Audit** – Auditing is the primary activity that is done to ensure that the Business Agreement is actually being enforced by the partners of the Federation.
 - **Liability** – When a Service Provider receives authentication information from a partner, it is up to the Service Provider to determine what authorization levels are to be provided. This means the Service Provider will be taking on the Liability of the Business Agreement.
- **Technologies** – Federation technologies have been around for awhile and are the easy part of a Federation solution. They include:
 - **Secure Access Markup Language (SAML)** – the open standard used for communicating authentication information
 - **Secure Provisioning Markup Language (SPML)** – SPML is the open standard used for communicating identity information across domains
 - **Web Services** – the move to Web Services means that the Federation of all sorts of information can now occur
 - **Services Oriented Architecture (SOA)** – rather than create a stand alone application, SOA architectures leverage Web Services so that the same Web Service can be used multiple times for similar services.;

4) Provisioning:

Complete Identity Management allow for the centralized management of all user identities and automate the creation, modification, suspension or deletion of user accounts and entitlements on all IT systems in the proper business processes with precision.

- **Password Management** – this involves the management of Password Policies across multiple Applications and resources
- **Password Synchronization** – Passwords Synchronization involves ensuring that passwords that are used for one Application is also used by other Applications. This usually means that passwords used have to be the lowest common requirements since a high security policy may not be possible across older systems;
- **Account management** – Account Management is the administration of Account information
 - **Self-service Administration** – rather than have the user call in to a Help Desk to change account information such as location, phone numbers, etc., Self Service Admin allows the User to administer their accounts on their own
 - **Delegated Administration** – Delegated Admin allows for a User to delegate their account admin to third parties;
- **Workflow management** – Workflow is an infrastructure that is put into place in order to automate business process such as procurement, HR, and IT management.
 - **Request Management** - Request Management involves the automating of processes that typically involve requests provided to Help Desks.
 - **Business Rules** – Business Rules engine is the core of workflow management where a set of rules is set up to control the workflow automation
- **Role management,**
 - **Role Based Access Control (RBAC)** – RBAC allows for a more efficient management of user access. Instead of having to change what a user can access, assign access to Roles that don't change and then change the assignment of a User to a Role. This results in one change rather than multiple roles.

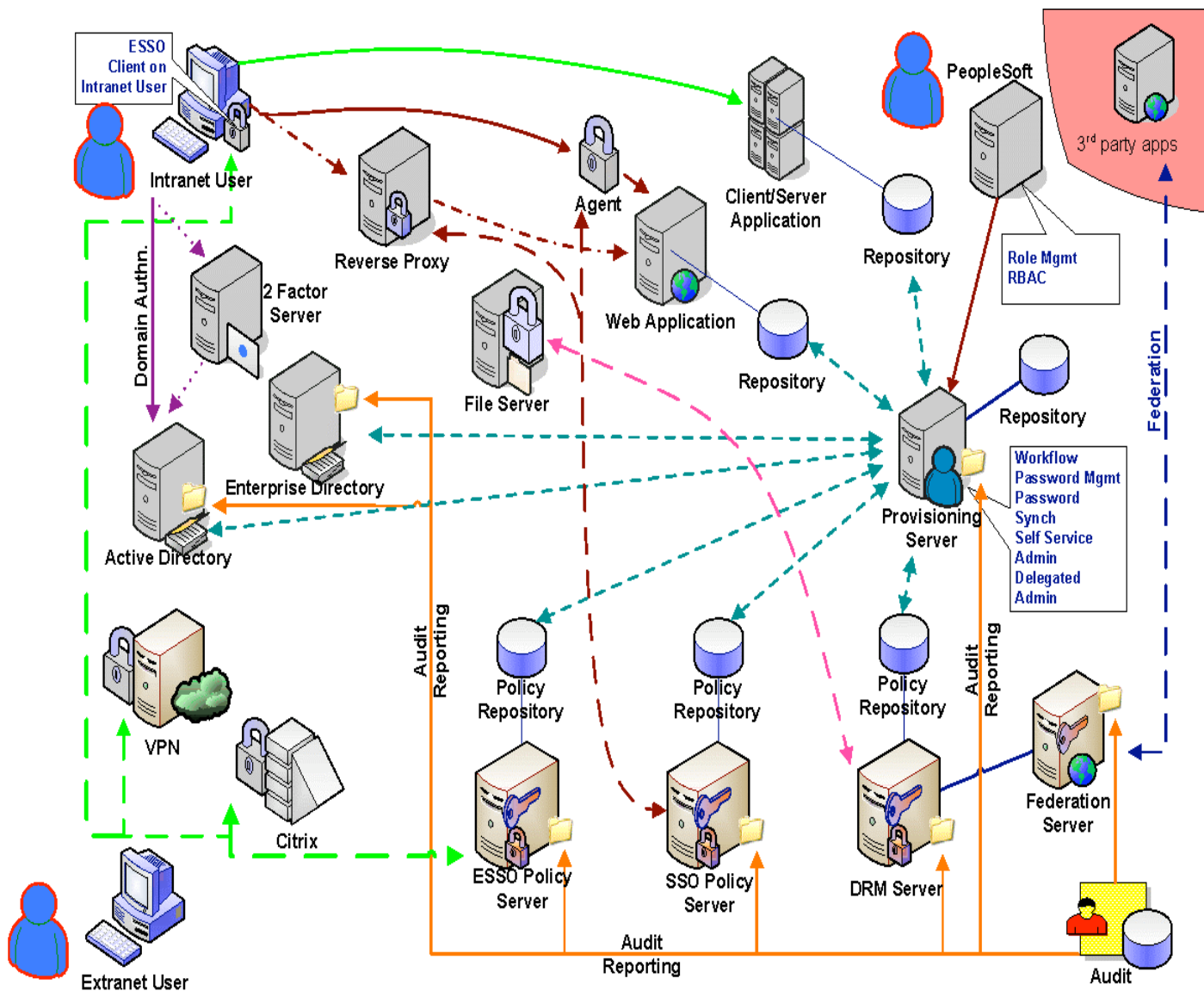
5) Logging, Auditing, reporting and compliance

This will be delivered across all the above 4 IAM areas (Data, SSO, User provisioning and Federation) to ensure accountability, traceability and compliancy.

The PDBS IAM delivery approach offers a unique combination of benefits to our clients including: comprehensive reach across applications, platforms and services, modular design based on industry best practices and common services, global scalability and compliance.

Reference Architecture

To successfully deliver the 5 key areas of IAM, a robust, cost-effective and scalable IAM reference architecture must be established to address any or all of the IAM areas. The following diagram depicts a typical IAM reference architecture for an enterprise:



Conclusion and Next Step

By using the Identity & Access Management (IAM) delivery approach and reference architecture described above, Enterprises can deliver a complete and proven IAM solution for protecting their IT assets across all platforms and environments. As a result, the Enterprise can deliver key benefits such as:

- reduced administrative costs
- improved user efficiency
- Enhanced End User experiences
- Improved regulatory compliance
- Reduced security risks
- Improved business enablement

For more information about how PDBS can help you with this integrated and comprehensive IAM solution and how you can achieve the ROI/Cost benefits through this IAM solution, please don't hesitate to call us at +1 (604) 948-9326 or visit us at www.pdbsec.com.