Identity and Access Management

An Introduction to IAM

Table of contents

Introduction

Single sign-on, Provisioning, Federation, Identity Integration, White Pages are only a few aspects of Identity and Access Management (IAM) that have become popular topics for discussion. Over the course of the over the last few years IAM has become a very popular topic for the media and industry experts alike, but what stills seems to be missing is a clear definition of what Identity and Access Management involves and why an organisation would look to implement its solutions. This document answers both of those questions.

This introduction to Identity and Access Management takes a strategic look at what IAM involves the core IAM solutions, the business drivers and benefits and then goes on to outline a strategic approach created and tested by experts at Dell SecureWorks.

What is identity and access management?

Put simply Identity and Access Management (IAM) is the combination of processes, technologies, and policies to manage digital identities and specify how they are used to provide access to information. As a broad IT issue spanning technological, regulatory and social issues, IAM has become a strategic imperative for all enterprises.

Identity and Access Management components

Identity Management is a catch-all phrase used to cover a range of Identity related technologies and processes. The following services are generally included in the scope of the term:

- **Core authentication services** – basically enterprise directories, the primary and connector stores for centralising identity information
- **Enterprise Single sign-on (SSO)** – lets a user log on once to a PC or network and access multiple applications and systems using a single password. Whilst this is frequently the ultimate goal for the IT department, this can be hard to achieve outside a pure web-based environment, and for all but the simplest or most tenacious of organisations should better be described as "Reduced sign-on", as the likelihood of achieving true SSO is remote.
- **User provisioning** – the creation/deletion of electronic identity and access rights, and the underpinning connectivity infrastructure, role-based authorisation views and business workflow that support the provisioning process.
- **Whitepages and self-service** – centralised password reset facilities, including "self-service", client-side password synchronisation, and enterprise information stores leveraging the underlying directory information to provide user information to the community – telephone numbers, desk location, organisational charts etc.
- **Extranet access management & federated identity** – extranet access management is often seen as web Single sign-on (web-SSO). Large-scale Extranet or eBusiness sites hinge on the definition of customer identity. The identification, access and authorisation of customer drives security and service, whilst the personalisation of customer experience drives satisfaction and retention. Federated Identity is (officially) the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains. It is now a commonly used term to describe the sharing of identity information between organisations in order

Business drivers for identity management

Distilling the generic drivers from the above common requirements provides a model for the business drivers behind Identity management. These are:

Business facilitation

To provide easier, faster access to enterprise information for customers, trading partners and employees, increasingly via the Internet, an appropriate security infrastructure must be provided. Key considerations are:

- Provide for customer self-registration, and portal personalisation
- Drive efficiency in outsourcing it administration and support
- Customer retention through improved service

Cost containment

The day-to-day activities of Identity-related security administration, as well as helpdesk costs associated with Identity are growing rapidly. Identity management solutions are one of the few areas within the information security program that can provide direct savings. Key considerations are:

- Reduce/avoid adding staff in security administration and/or helpdesk
- Develop a common iam architecture for leverage across major it projects
- Better manage non-it services, eg. Pagers and mobile phones

Operational efficiency & agility

Efficiencies are produced through the reduction of the time taken to execute access and provisioning requests and through improvements to user service. This efficient management of digital identity also delivers the agility that large businesses need to integrate the IT of new acquisitions and to facilitate flexible team working. Key considerations are:

- Improve service-level agreements
- Achieve productivity savings through reduced time to access required resources
- Improve user convenience through self-service
- Centralisation of identity audit for security administration reporting

Risk management and regulatory compliance

Internal security risk must be managed and mitigated. Beyond that, proving the security of the organisations access control infrastructure is not only important for security managers in order to understand the effectiveness of their controls, but also implementation and enforcement of regulatory requirements is a “must do” for many organisations.

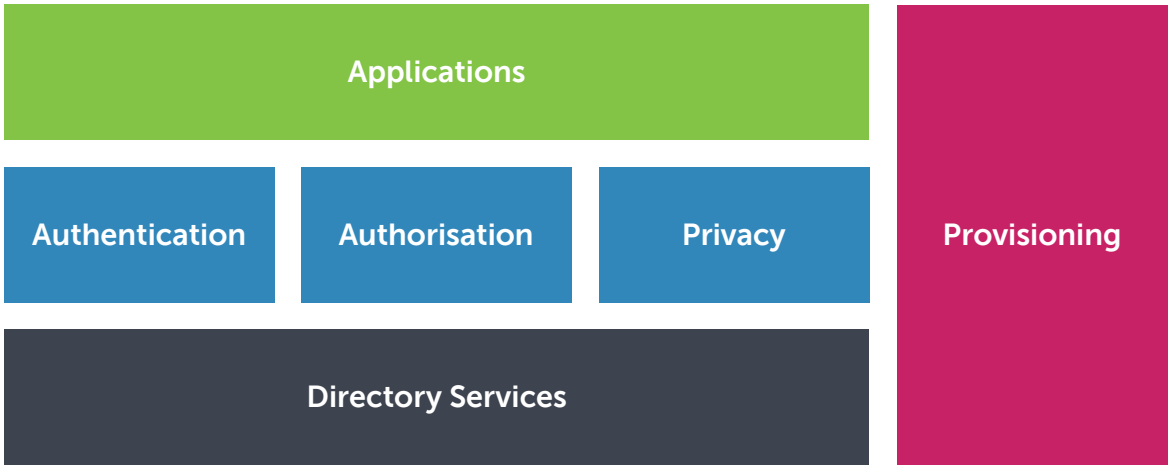
Applicability of IAM technology solutions to business drivers

	Business facilitation	Cost containment	Operational efficiency	IT risk management	Regulatory compliance
Core authentication services	✓	✓		✓	✓
Enterprise single sign-on	✓	✓	✓		
User provisioning	✓	✓	✓	✓	✓
White pages & self sevice	✓	✓	✓		
Extranet access management & federation	✓	✓	✓	✓	✓

Identity Framework

In order to understand IAM, and to develop a strategy for Identity Management in your organisation, it is first necessary to lay out a set of architectural building blocks and principles upon which Identity Services are constructed. This is embodied as the "Identity Framework", a conceptual component architecture that defines and describes various interdependent technologies and processes that together provide a unified view of an organisation's user identities, roles, and entitlements.

Under the umbrella of identity and access management, these technologies include authentication, authorisation, provisioning systems, directories, and metadirectories. This framework approach defines strategic elements of Identity Management, which in turn delivers a number of critical benefits to organisations:



The following section lays out the components of this framework.

Directory services

Directory services provide the foundation of the identity framework. In the context of this Identity Framework, "directory services" refer to all strategically important sources of digital identity information. This will mean not just the core LAN Directory infrastructure in an organisation, but also other authentication platforms and sources of user profile information such as the Telephone address list, the CRM system and identity stores used to deliver customer-facing Extranet platforms.

A centralised identity service, therefore, does not mean that all information is contained in a central location; only that it is managed centrally. The IT systems that drive relevant business processes in HR, the IT helpdesk and the e-business teams still remain, but are integrated for management and security purposes. The solution to integrating these different sources of identity information in the organisation is to use a metadirectory.

A metadirectory helps create a singular view of isolated identity information located in multiple identity stores. The metadirectory pulls user information from a variety of authoritative sources such as HR and accounting applications, e-mail directories, and customer-facing e-commerce registration databases. It then populates its database to create this view. Most importantly, metadirectories synchronise the attributes that each authoritative source provides throughout the organisation.

Authentication

The authentication process provides the user entry point to an identity and access management framework. Authentication is the act of proving a digital identity of a user or object to a network, application, or resource.

Effective identity and access management strategies deploy a centralised authentication framework to simplify the user experience and reduce administration overhead. For these reasons, this component of the framework must support both legacy and e-business environments.

Much of the current media focus on Identity Management is on the concept of Single sign-on. This is discussed and explained below.

Single sign-on

The term single sign-on (SSO) encompasses many things to many individuals, but in general outline there are five ways of achieving this:

- **True single sign-on** – There is only a single identity used and stored with a single password (or other authentication signature such as a certificate, key, biometric etc) in a distributed database such as an LDAP directory and used by all internal infrastructure, systems and applications to authenticate and authorise the user's access to systems.
- **Enterprise single sign-on** (esso or server cache sso) – It is these technologies that the media tend to refer to in discussing SSO. Technologies that provide these services have a number of subtly different approaches to achieving the same goal, but in general terms, an agent on each customer computer retrieves the usernames and passwords, and automatically fills in the dialog boxes of applications and systems which require login credentials. There are a specific class of problems with these solutions which occur when the passwords stored in the repository get out of sync with those stored in the applications.

- Web single sign-on (web-sso) - This technology is limited to only those applications which present a web interface. By declaring other applications "out-of-scope" and concentrating on this particular problem, it is relatively straightforward to solve. It is also possible with these solutions to extend the SSO nature in such a way that the user logs on to their desktop computer and is never presented with a web login dialog for any web enabled applications after that point. The technology relies on web-agents which intercept the log-on requests and store encrypted state information in browser based cookies which are intercepted by the web agents on other web servers.

Consistent sign-on (CSO)

Whenever credentials are requested by an application, the user only has to remember one set of credentials as they are the same for every application. When both the username and the password are exactly the same for every application, this is true consistent sign-on. When the password is consistent but the usernames are different, this is less desirable but still useful.

Building CSO systems consists of 2 parts:

1. **Normalising the identities** - That is, performing synchronisation for the identity data across the identity repositories to make the usernames the same in each system. Technically, this is not particularly difficult to do. The challenges are more to do with the identities that already exist and whether the system in question supports the renaming of identities. These therefore tend to be operational issues rather than technical challenges.

2. **Password synchronisation** - Most systems do not store passwords as plain text in readily readable databases. The passwords are invariably encrypted. To retrieve the plain text password from one system in order to be able to re-encrypt it for another system is not possible. Hence agents must be installed on a single "primary authentication system" (most often Active Directory). The agents trap the passwords while in plain-text and use a password-synch service to re-write them to other application in real or near-real time. Usually a small number of systems will be left out of scope for these projects because their password policies are incompatible. For example if one system has a minimum password length of 10 characters, yet another system has a maximum password length of 9 characters. The 2 criteria are mutually exclusive. The technology is capable of providing a solution, but the policies of the system prevent it from being deployed. This technology is the same as that used to effect self-service password resets, and it would be expected that any password synch IT project would deliver self-service as at least an adjunct to the main project.

There are a few instances where consistent sign-on is not possible, but by and large, these are fast, cheap and easy systems to deploy, and bring tremendous value to organisations.

Reduced sign-on (RSO)

This is a much more realistic and achievable goal. By deploying a mixture of Consistent Sign and SSO (such as web-SSO and perhaps Windows SSO side-by-side), the total number of logins that has to be performed by any single user is reduced. Therefore the need to remember many passwords is reduced, and hence help desk call volumes are reduced.

Developing ROI from SSO projects

In terms of hard Return on Investment (ROI), CSO projects are generally considered to be considerably more reliable and measurable than SSO and RSO projects. They have additional advantages in that some of the core infrastructure required to deliver these solutions (metadirectories), are also used in RSO and SSO projects. They also enable the streamlining of other business processes such as provisioning, de- provisioning, attribute sync, attribute mastery, identity data convergence and brokering of identity data.

When thinking about the generalised problem of sign-on, it helps to think in more strategic terms about Identity Management.

Authorisation

Authorisation is the process of determining whether a digital identity is allowed to perform a requested action. Authorisation occurs after authentication, and uses attributes associated with the digital identity to derive entitlements defining what resources the digital identity can access. The most common authorisation mechanism is an Access Control List (ACL).

However, many systems use the term role to refer to a user classification. For example, a "Manager" role could be used to refer to all members of a security group called "Finance Managers", who as members in this group would automatically be granted the entitlements to network resources this role provides. However, roles can also be based on dynamic, run-time decisions that provide more flexibility.

Use of roles to define the digital profile of a user within an organisation allows the IT department to flexibly provision the digital identity across multiple systems, and apply the correct authorisations to that identity, centrally and through a single action. Furthermore, the concept of role allows auditing of a user's access across the suite of systems and applications that provide access to the organisation's data.

Privacy

Not a service in its own right, but a key attribute of an Identity and Access management platform, privacy is a fundamental concern across all elements of identity design and implementation. The UK Data Privacy laws demand careful storage of all employee and customer personal information, and individual digital identity attributes may provide an attacker with important information on an organisation and its systems.

Federation

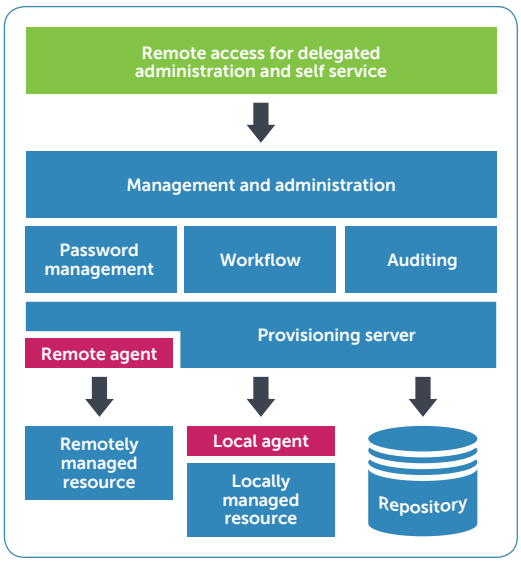
The concept of federation is becoming more important as organisations continue to share resources with their business partners. Federation is the secure authentication and authorisation of digital identities between autonomous information systems through the principle of trust. For example, a user from company A can use information available at company B because there is a trust relationship between companies A and B.

At a high level, trust relationships simply provide a way to authenticate digital identities between autonomous organisations. The mechanisms of trust, however, become very complicated because there are many tasks that must happen between independent organisations to make the authentication and subsequent authorisation processes truly useful. The trusting organisation needs to have a secure mechanism to communicate with the trusted organisation. Once the trusting organisation has authenticated the foreign digital identity, it incorporates the entitlement information about that account into the authorisation process within the trusting organisation. This type of lookup is an authenticated and authorised action that must be routed to the correct authoritative owner of the referenced digital identity.

Provisioning

Provisioning is frequently used as a catch-all term to cover:

- **User provisioning** – the creation of electronic identity and access rights; creating accounts, setting access privileges and controlling policy across a diverse collection of systems
- **User management** – keeping track of changes in user status and modifying entitlements appropriately, including password management
- **User de-provisioning** – the removal of the electronic identity, generally when the employee has left the organisation



Provisioning software is therefore generally an integrated set of tools used to manage the lifecycle of user entitlements. The focus of such toolsets is generally on the automation of life cycle management, audit and reporting, and "who has access to what". Provisioning software can also be used to manage non-IT assets, such as mobile phones, corporate credit card, business cards, and many other items.

Applications

Applications are the ultimate consumers of identity and access information. Because of this, they should be integrated with the identity and access management framework.

Applications typically integrate with the authentication and authorisation components of the framework through application programming interfaces (APIs). Applications that fail to become integrated with the framework add to the complexity of the identity and access management solution. This failure to integrate often creates new attack surfaces, which lead in turn to security vulnerabilities.

Integrating applications requires the largest amount of effort in implementing an identity management solution, but this integration process also represents the highest return on investment (ROI). If an application has been designed with its own authentication system, the only way an organisation can fully integrate the application into the authentication process is to redesign the application to work with the system platform. Therefore, to ensure application compatibility with the identity management framework, an organisation's software development partners and 3rd party application integrators must be given clear guidelines on how applications must incorporate authentication and authorisation functionality.

The cost of managing a separate directory is negated through the use of the Identity Management solution, which provides Identity aggregation and provisioning services across its connected Identity infrastructure.

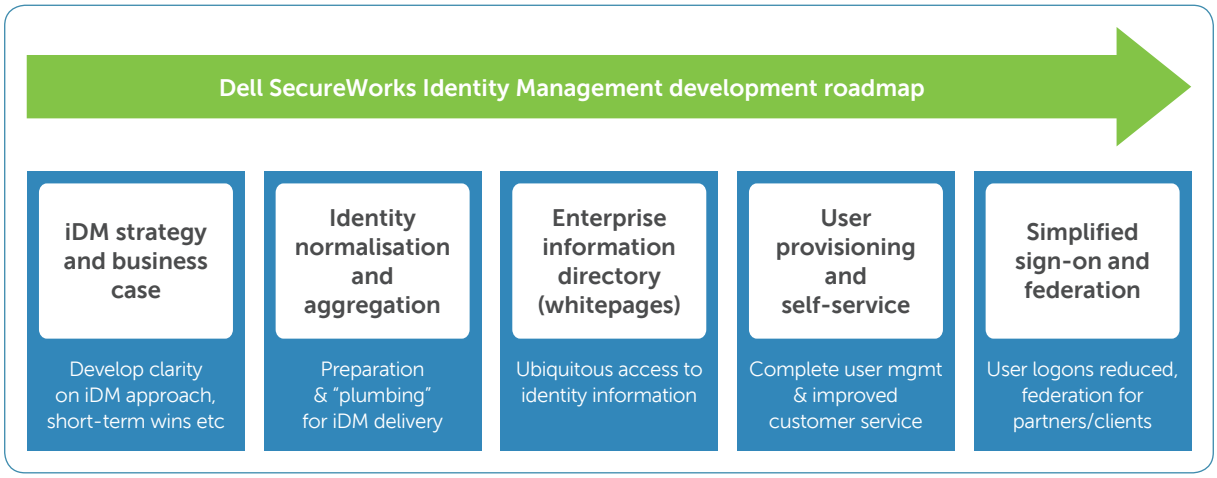
Developing an identity management strategy

Objectives and benefits

All (good) strategies start with the end goals in mind. For example, in Identity Management, these might be initially driven from the perceived (or regulatory-imposed) need to improve security and protect key corporate applications and information assets. However, the drivers for other members of the organisation may be different – cost-reduction through centralisation, or the exposure of corporate or customer identity through federation to leverage new projects, services or business opportunities. Understanding these drivers in full, and achieving buy-in across the business is critical to the success of Identity Management projects, as the process & technology implemented will cross many boundaries.

Eating the elephant

Having helped many organisations to understand what Identity Management means to them, and how investment in IAM process and technology might deliver ROI for them, Dell SecureWorks have developed a trademarked approach and engagement to make this process simpler, easier and more cost effective to deliver.



Dell SecureWorks undertake a consultancy exercise to examine the identity services underlying a range of key systems and functions in the customer organisation, in order to understand where issues and costs in managing identity currently sit, and where pressure points will arise in the future through the introduction of key new systems. In addition, the user management workflow across these key existing systems and applications is examined in order to understand the efficiency of this workflow in the current environment.

From this analysis a set of options and recommendations for developing Identity Management in the customer organisation is created and presented, and from which in turn a strategy is agreed and presented as the final deliverable of this undertaking. The engagement typically takes between four to six weeks to complete.

Whilst every organisation will have their own individual requirements, timescales and business drivers, Dell SecureWorks have developed a model for Identity Management projects that leverage our extensive experience in this field and provides a platform for consistent and early delivery of quantifiable business benefit whilst working towards a clear, strategic end-goal.

Summary

Why look to implement identity management solutions? In short, to improve security, save money and make your business more efficient. In more detail, the business case for the development of an identity management strategy is generally seen as originating in some or all of the following:

1. **Risk management** – intuitively, this includes the protection of resources, the mitigation of risk and regulatory compliance. However, security also involves softer and less quantifiable benefits such as brand protection, risk management of company image, and consistency in user experience.
2. **Operational efficiency & agility** – improving service levels to the business (and thereby increasing user satisfaction), delivering productivity improvements, increased adaptability to business change and decreased cycle times.
3. **Cost containment** – reducing or capping administrative headcount despite increased business complexity, reducing IT project cost through common IAM architecture and integrating management of non-IT assets into user lifecycle management (eg. phones or desktop equipment)
4. **Business facilitation** – comes from two angles; firstly improving and centralising business process to facilitate outsourcing, and secondly facilitating customer management and retention through self-registration, portal services and personalisation
5. **Regulatory compliance** – investment in IAM is a necessary plank of regulatory compliance for many industries, most notably Financial Services and the Public Sector.