Chapter 2 Identity Management

"Identity management, user provisioning and single sign on are the top three priorities of IT spending in Fortune 1000 companies."

"Digital identity is one of the fundamental building blocks for the next generation of information systems."
— Tony Scott, CTO of General Motors

"The increasingly distributed nature of corporate networks, the proliferation of Web-based applications, increased security awareness, and government regulations such as Sarbanes-Oxley & HIPAA have contributed to making Identity Management a necessity for virtually every business."
— Roberta Witty, Research Director, Gartner, Inc.
Identity management is one of the three key areas in which HP is investing to create innovation and differentiation. Within the HP security framework, identity management is supported by processes and tools that allow administrators to manage large populations of users, applications, and systems quickly and easily. In addition, business policies, regulatory compliance, and risk factors shape the policies and practices that direct identity management.

Figure 2–1
Identity Management

This chapter begins by providing the definition and purpose of identity management. Next, it presents background information, including identity data management, identity management components, and key elements of identity management solutions. The final section of the chapter discusses the specific identity management capabilities that HP delivers.

**Definition**

Identity management is the set of processes, tools, and social contracts surrounding the creation, maintenance, and use of digital identities for people, systems, and services. It enables secure access to a set of systems and applications. Its components include data repositories, security, life cycle management, consumables, and management policies. Identity management has strong links to security, trust, and privacy management. It also delivers components of risk management.

Traditionally, identity management has been a core component of system security environments. It is used for maintaining account information and controlling access to a system or limited set of applications. Control is usually the primary focus of identity management. For example, an administrator issues accounts to restrict and monitor access to resources. More recently, however, identity management has also become a key enabler of electronic business.

**Purpose**

Identity management combines processes and technologies to secure and manage access to an organization’s resources. In addition, it identifies every user, application, or device throughout and across organizations over time. Identity management provides flexible authentication, access control, and auditing while respecting privacy and regulatory controls. Today, identity management systems are fundamental to establishing accountability in business relationships, customizing the user experience, protecting privacy, and adhering to regulations.
The following list provides examples of the primary goals that drive organizations to implement identity management solutions:

- Reduce total cost of ownership (TCO) for all systems, including the costs of administration, help desk, and technical support
- Reduce management overhead
- Provide competitive advantage by enabling automation and streamlining optimization of business processes
- Improve customer and employee service, and maintain the control and confidentiality of customers, suppliers, and employees
- Reduce the time for new employees to gain access to required organizational resources
- Reduce the risk of using incorrect information for business processes
- Reduce the risk of former employees retaining access to organizational resources
- Support legal and compliance initiatives related to employee and customer data, for example, the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, the EU Directive on Data Protection, the Basel II Accord, and the Canadian Privacy Act

In short, the purpose of identity management is to provide organizations with the following key benefits:

- Enhanced enterprise agility and productivity
- Increased IT management efficiency, including cost reduction
- Effective regulatory compliance

Figure 2-2
Identity Content
What is a Digital Identity?

Identity is a complicated concept with many nuances that range from the philosophical to the practical. In the context of identity management, however, the identity of an individual is the set of information known about that person. In the digital world, a person's identity is typically referred to as a digital identity. Different contexts, roles, affiliations, and application environments can require different levels of assurance and digital identities. Therefore, a person can have multiple digital identities.

Although digital identities are predominantly associated with humans, they will be increasingly associated with non-human entities (services, systems, and devices) that could act on behalf of people. Specific examples include trusted platforms, next-generation mobile phones, and Digital Rights Management (DRM)-based devices.

Figure 2–2 on the previous page illustrates the content of a digital identity. Identity consists of a person's unique profile data, identifier data, and authentication and authorization data. Each content piece can be linked to different contexts (company, web, and application) and the person’s role in that context.

Managing Identity Data

Metadata qualify all identity data, and an organization’s policies for identity, authentication, authorization, and privacy protection define the metadata requirements. Policies are defined by an organization’s IT and business decision makers—they are aligned with corporate governance rules, regulatory restrictions, and contractual obligations specific to the organization’s operating environment.

Identity information and related policies can change over time. This means that identity management not only deals with static information but also copes with changes to identity data. The same is true for security policy management.

Figure 2-3
Identity Views and Contexts (Subject’s Perspective)
Multiple Views and Contexts

Identity information can have multiple views. Each view defines a digital identity that is valid and appropriate based on the context or purpose. Using multiple views within and across multiple contexts enables interactions and transactions. Examples of different views and contexts are illustrated in Figure 2–3.

Different stakeholders can disclose, access, and use digital identities in one or more contexts, including personal, social, e-commerce, enterprise, and government. The process occurs through a variety of means including personal appliances, enterprise systems, and web services.

Multiple Levels of Awareness and Control

From the viewpoint of identity subjects, identity information has several levels of awareness and control:

- **Me** Me is the part of identity information that the subject is aware of and directly controls. An example is personal address information stored and maintained in an organization’s white pages directory. It can also include personal or private information—such as a credit card number or Social Security number—that an individual carefully protects and reveals only in particular circumstances.

- **Known Me** is the part of identity information that the subject is aware of and indirectly controls. An example is an individual’s revenue data and associated tax levels that are stored in the tax department’s database. Even though an individual provides the revenue data to the tax department, he or she doesn’t have direct control of the content in the database.

- **Unknown Me** is the part of identity information that the subject is not aware of and cannot control. Other stakeholders, which may be known by the subject, can control this information. Examples include Certification Authorities (CAs), authorized e-commerce sites, Trusted Third Parties (TTPs), and unknown third parties (for example, credit rating agencies and identity thieves).

Identity Management Components

Identity management solutions are modular and composed of multiple service and system components. This section outlines the components of an example identity management solution, as illustrated in Figure 2–4.

![Identity Management Components Diagram](image-url)
Components of identity management solutions exist at different maturity stages. Components like authentication and directories are quite mature and are considered consolidated technologies. Provisioning, authorization, and single sign-on (SSO) are rapidly consolidating. Others, such as privacy and longevity, are still in a definition and research stage.

Data Repository Components

Directory services and meta-directories deal with the representation, storage, and management of identity and profiling information. They provide standard Application Program Interfaces (APIs) and protocols for information access. Data repositories are often implemented as a Lightweight Directory Access Protocol (LDAP)-accessible directory, meta-directory, or virtual directory. Other repositories that are used in the context of identity management solutions are databases and XML-formatted files. Policy information, which governs access to and use of information in the repository, is generally stored in these repositories as well.

Security Components

Authentication providers, sometimes referred to as identity providers, are responsible for performing the primary authentication that links an individual to a given identity. The authentication provider produces an authenticator—a token allowing other components to recognize that primary authentication has been performed.

Primary authentication techniques include mechanisms such as password verification, proximity token verification, smart card verification, biometric scans, and even X.509 public-key infrastructure (PKI) certificate verification. Each identity may be associated with multiple authentication providers. In addition, the mechanisms employed by each provider may be of different strengths. To accept the claim of a given identity, some application contexts may require a minimum level of strength.

Authorization providers enforce access control when an entity accesses an IT resource. Authorization providers allow applications to make authorization and other policy decisions based on privilege and policy information stored in the data repository. An authorization provider can support simple access control management at the operating system (OS) level. It can also support sophisticated controls at the application and service levels.

Auditing providers supply the mechanism to track how information in the data repository is created, modified, and used. This is an essential enabler of forensic analysis, which helps determine who circumvented policy controls and how the controls were evaded.

Life Cycle Components

Provisioning is the automation of all the procedures and tools used to manage the life cycle of an identity. Provisioning procedures include:

• Creating the identifier for an identity
• Linking to authentication providers
• Setting and changing attributes and privileges
• Decommissioning an identity

In large systems, provisioning tools generally permit some form of self-service for creating and maintaining an identity. They frequently use a workflow or transactional system to verify data from an appropriate authority. The tools may also propagate data to affiliated systems that may not directly consume the repository.
Identity Management tools create the historical record of an identity. These tools allow the examination of the evolution of an identity over time. Longevity is linked to the concept of attestation—the ability to determine which “actors” had access to which resources and in what timeframe (irrespective of whether they exercised access, which is a matter of auditing).

Consumable Value Components

Single sign-on (SSO) allows a user to perform a single primary authentication for access to the set of applications and systems in the identity management environment.

Personalization and preference management tools associate an identity with application-specific and generic information. These tools allow applications to tailor the user experience, streamline the user interface, and target information dissemination for a business.

Self-service enables users to self-register for access to business services and manage profile information without administrator intervention. It also allows users to manage authentication credentials; for example, assigning passwords, resetting passwords, and requesting X.509 PKI certificates. Self-service reduces IT operation costs, improves customer service, and improves information consistency and accuracy.

Management Components

User management provides IT administrators with a centralized infrastructure for managing user profile and preference information. User management enables organizations to decrease overall IT costs through directory optimization and profile synchronization. These tools provide user self-service capabilities and enhance the value of an organization’s existing IT investments.

Access management provides IT administrators with a centralized infrastructure for managing user authentication and authorization. An access control management service increases security, reduces complexity, and reduces overall IT costs by automating access policies for employees, customers, and partners.

Privacy management assures that identity management solutions respect privacy and data protection policies as defined in company, industry, and governmental regulations.

Federation management establishes trusted relationships between distributed identity providers. This often involves sharing web service endpoints, X.509 PKI certificates, and supported/desired authentication mechanisms.

The Effect of Policies on Management Components

Policy controls govern and drive management components. Policies may cause events to be audited or an identity subject to be notified when information is accessed.

- **Identity policies** control the format and lifetime of an identity and its attributes.
- **Authentication policies** control the characteristics and quality requirements of authentication credentials.
- **Authorization policies** determine how resources can be accessed.
- **Privacy policies** govern how identity information may be disclosed.
- **Provisioning policies** determine what resources are allocated to which identities and how the resources are allocated and deallocated.
Key Elements of Identity Management Solutions

Today, there are many products and solutions available in the identity management market. They generally provide one or more of the identity management components and target different types of users and contexts, including e-commerce sites, service providers, enterprises, and government institutions. Key IT industry players are currently focusing on creating identity management suites that provide all of the components shown in Figure 2–4.

There is a considerable amount of overlap between the different solution categories available on the market. A good example is meta-directories and provisioning solutions. The role of meta-directories has gradually shifted from pure data synchronization (a repository function) to life cycle component functions for the creation of user entries (a provisioning function).

Identity management solutions also involve other stakeholders. These include authentication devices (smart cards, biometric devices, and authentication tokens); anonymity services; cryptographic alternatives to RSA-based cryptographic schemes (Identifier Based Encryption [IBE] and trusted platforms); and the standards outlined in the next section.

The quality of identity management products and solutions depends on how successfully they handle a number of factors. Among other things, these factors include keeping identity information in a consistent and up-to-date state, satisfying related management policies and legal requirements, preserving privacy and trust, and ensuring that security requirements are fulfilled.

The key elements to consider in an identity management solution include:

• Adherence to identity management standards
• Types of deployment models
• Means of addressing complexity and competing demands
• Methods of safe digital identity management
• Level of product interoperability

Identity Management Standards

Standards provide a common set of protocols, semantics, and processing rules that allow the various components of an identity management solution to interoperate. Table 2–1 provides an overview of the most important current and emerging standards used in an identity management architecture.

Deployment Models

Identity management systems are primarily deployed in one of three models: silos, walled gardens, or federations.

Silos are the predominant model on the Internet today. In this model, the identity management environment is established and operated by a single entity for a fixed user and resource community. A good example is a Microsoft® Windows® domain governed by a set of predefined administrators and domain controller servers.

Walled gardens represent a closed community of organizations. A single identity management system serves the common user community of a collection of businesses. Most frequently, this occurs in business-to-business exchanges, and specific rules govern the entity operating the identity management system. A good example is the Identrus PKI, which brings together individual bank-level PKIs into a closed banking-community PKI.
### Table 2–1
Relevant Standards for Identity Management Architectures

<table>
<thead>
<tr>
<th>Type</th>
<th>Relevant Standards</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISO/ITU x.500</td>
<td><a href="http://www.itu.int">www.itu.int</a></td>
</tr>
<tr>
<td>Authentication Mechanisms</td>
<td>Standardized authentication protocols: Kerberos, SSL/TLS, Public Key Infrastructure (PKI)</td>
<td><a href="http://www.openauthentication.org">www.openauthentication.org</a></td>
</tr>
<tr>
<td></td>
<td>Open Authentication Initiative</td>
<td></td>
</tr>
<tr>
<td>Privacy Standards</td>
<td>Platform for Privacy Preferences (P3P)</td>
<td><a href="http://www.w3.org/P3P">www.w3.org/P3P</a></td>
</tr>
<tr>
<td></td>
<td>Liberty Alliance Standards</td>
<td><a href="http://www.projectliberty.org">www.projectliberty.org</a></td>
</tr>
</tbody>
</table>

**Federations** and federated identity management environments are emerging deployment models. They include systems like the Liberty Alliance Project (endorsed by HP) and systems built on the Web Services Security (WS-Security) standards, the development of which is driven by Microsoft Corporation and IBM Corporation.

The central difference between federated identity management systems and walled gardens is that a single entity operates a walled garden. By contrast, federated systems support multiple identity providers and a distributed and partitioned store for identity information. Clear operating rules govern the various participants in a federation—both the operators of components and the operators of services rely on the information provided by the identity management system. Most systems exhibit strong end-user controls over the dissemination of identity information to members of the federation.

**Complexity and Competing Demands**

The current identity management landscape is very complex because of the multiple interests, perspectives, concerns, and technologies that are involved. Identity management is important in different contexts, including enterprise, e-commerce, and government. It supports business processes and services, and it enables digital interactions and transactions.

There are competing demands on what identity management should provide, differing concerns about its focus, and conflicting interests. Examples of competing demands include enterprise focus versus consumer focus, mobility versus centralization, legislation versus self-regulation, subjects' control versus organizations' control, and privacy versus free market.

**Numerous Stakeholders**

Demands are dictated by various stakeholders, which can include enterprises, e-commerce sites, service providers, government agencies, and identity subjects (consumers). Stakeholders have different objectives and priorities when dealing with the management of digital identities:

- **Enterprises** are driven by their business objectives and needs. They manage large sets of identity data to enable their businesses, rationalize their assets, simplify interactions with partners and customers, ensure regulatory compliance, and meet contractual obligations. Identity data also helps enterprises manage the information life cycle of their workforce and manage access to enterprise resources.
• **E-commerce sites and service providers** manage consumers’ identity information to achieve a variety of goals, such as increasing sales, understanding customers’ needs, customizing services, and selling information to third parties.

• **Government agencies** are concerned with the control and protection of their citizens’ personal information. They also seek strong and undeniable authentication mechanisms and the automation and rationalization of their services via the web and the Internet.

• **Consumers** have different concerns and needs depending on the role they play. They are in the middle (or, depending on the point of view, the source) of most of the competing demands previously noted. As employees or consumers, they want to access and use services in the simplest and most efficient way. Private citizens’ needs and concerns might include privacy, distrust of institutions, and the accountability of the involved parties.

This variety of interests and concerns, along with emerging technologies, increases the complexity of identity management. All of these aspects influence each other, via a spiral of potentially conflicting requirements. For example, new legislation addresses citizens’ needs for privacy; however, it constrains how enterprises, service providers, and e-commerce sites process personal information.

**Multiple Domains**

Multiple domains can also increase the complexity of identity management. Business tasks, digital interactions, and digital transactions can span multiple domains. In an e-commerce context, for example, a digital transaction might require the involvement of identity e-commerce sites and the exchange of identity information among these sites. This exchange has strong implications for managing trust, privacy, authentication, authorization, and accountability. Business-to-business interactions and transactions within supply-chain communities face similar challenges as a result of multiple domains.

**Fragmented Implementation**

Further complexity derives from the challenge of installing, configuring, administering, and integrating current identity management products. This is mainly due to the fragmentation of identity management components and the lack of interoperability and standards. This complexity creates frustration and delays the adoption of identity management solutions in the IT environment.

**Safe Digital Identity Management**

Identity management systems bring great value to the digital world. Federated identity environments, in particular, hold promise for widespread deployment. As the distinction between real-world identity and digital identity blurs, however, methods of safe digital identity management need to be considered:

• **Authenticity of identity.** How is the accuracy and validity of identity information measured and determined? What trust services are necessary to generate confidence in information in the identity management system?

• **Longevity of information.** Do identity management systems adequately track changes to identity information over time? Do they maintain the necessary artifacts to support historical investigations?

• **Privacy.** Do identity management systems provide adequate controls to preserve individual privacy? Does the system provide adequate support for anonymity and multiple user-controlled personas?

• **Identity theft.** Do widespread identity management systems make it easier to perpetrate identity theft or identity fraud?

• **Legal structures.** What protections exist for the holder of the identity or the relying party? Do these protections go beyond contractual obligations when digital identity systems are used for interactions that are limited to the physical world today?
Product Interoperability Challenges

Most of the current identity management products and solutions rely on self-contained, standalone management and control tools. Little integration or interoperability is available with other management tools to deal with the management of security, trust, and privacy in an orchestrated way. To react to changes, identity management products and solutions need to evolve toward higher levels of interoperability, flexibility, and capability.

Summary of Identity Management Concepts

From a technological and IT perspective, identity management is just one aspect of managing business solutions and the overall IT stack of networks, platforms, OSs, applications, middleware, and services. Identity management must be considered in a holistic way by including the management of security, trust, and privacy along with the management of policies, requirements, and changes. All of these aspects are interrelated and affect business solutions and the IT stack at different levels of abstraction.

The components within the identity management landscape are rapidly changing. Classic identity management components are consolidating. On the other hand, new components and standards are emerging, such as identity federations, identity for web services, and privacy.

Identity management is also gaining importance. Future identity management solutions will play a more central role in the IT industry due to the pervasiveness and the increased presence of identity information in all components of the IT stack.

HP Identity Management Products and Solutions

For HP, identity management is the ability to:

• Identify every user, application, and device throughout and across organizations over time
• Provide flexible authentication, access control, and auditing technologies, while respecting privacy and regulatory controls
• Bring management capabilities to individuals, small organizations, and large organizations via easy-to-use and understandable tools that cope with dynamic populations and business changes

Considering the above definition, HP's identity management vision is clearly centered on the pervasiveness of identity management technologies and solutions:

• Identity management is about the management of user, application, and device identities.
• Identity management is about the management of identities in different contexts: enterprises, small and medium businesses (SMBs), and consumers.
• Identity management deals with the management of the entire life cycle of identities and their attributes.

The following sections explore the identity management solutions HP provides to build identity management services for IT infrastructures. We will address identity repositories, security components, privacy management, identity life cycle management, and federated identity management. All of these building blocks are fundamental pieces of the solutions rooted in HP's identity management vision.

Identity Repositories

Directories are the most commonly used repositories for storing identity-related information. As mentioned previously, identity management solutions can incorporate other repositories, including SQL-rooted databases and XML-formatted files.
Types of Directory-Based Identity Repositories

Different technological approaches exist for directory-based identity repositories: centralized enterprise directories, directory synchronization utilities, meta-directories, and virtual directories. Of these, only a centralized enterprise directory is a true identity repository. The other tools integrate and link different identity repositories.

- **Enterprise directories** are a single authoritative source for identity information throughout an enterprise. All users and directory-enabled applications rely on the identities stored in the enterprise directory. This is the ideal scenario. However, most enterprises cannot use this approach due to the presence of legacy directories.

- **Meta-directories** provide a consolidated view of the identity data stored in different repositories. They also synchronize the data in the different repositories. A meta-directory resembles an advanced directory synchronization utility. Most meta-directory solutions come with workflow logic, and they overlap with many of today’s identity provisioning solutions.

- **Directory synchronization utilities** are intelligent LDAP-based utilities that can synchronize identity data between different types of identity repositories—such as directories, databases, and the repositories linked to enterprise resource planning (ERP) systems.

- **Virtual directories**, unlike meta-directories, do not build a central repository. Instead, they rely on directory server or client functions to access the data stored in different directory sources. Virtual directories also allow for the creation of different application-specific views of directory data.

<table>
<thead>
<tr>
<th>Table 2–2 Directory Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
</tr>
<tr>
<td>Enterprise Directory</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Meta-Directory</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Directory Synchronization</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**HP and Identity Repositories**

HP considers directory identity repositories a mature market and uses a best-of-breed and end-user preference approach. Additionally, numerous applications offer LDAP access to their user (identity) tables such as Resource Access Control Facility (RACF) and Lotus Notes. Table 2–2 gives a non-exhaustive overview of directory solutions.
Security Components

This section discusses the triple-A components of an identity management solution: authentication, authorization, and auditing services. It provides details about the solutions HP offers in this space.

Authentication Technologies

Authentication is the process of verifying an entity’s identity. Authorization credentials, which are uniquely linked to an entity, are typically used for verification. The security quality of authentication technologies largely depends on the following dynamics: the number of authentication factors, the authentication protocol, and the authentication method.

Multi-factor authentication methods offer higher security quality than single-factor authentication methods. A good example of a multi-factor authentication system is a smart card. It combines possession (of the card) and knowledge (of the card’s PIN). Table 2–3 gives an overview of different authentication methods and the number of authentication factors they support.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Password or PIN</th>
<th>Smart Card or Token</th>
<th>Biometric Device</th>
<th>Biometric Device and Smart Card</th>
<th>Dial Back</th>
<th>Trusted Platform Module (TPM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Possession</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Biometric Data</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Many identity management solutions require the authentication infrastructure to support multiple authentication methods and protocols. This may be necessary when the environment supports internal and external users that access a variety of resources. When resources hold different values or contain sensitive information, different methods and protocols may also be necessary. Access to confidential information, for example, may require a stronger authentication method than access to information published on a corporate intranet. In some authentication infrastructures, this feature is known as graded authentication. This simply means that the resources and information a user is allowed to access vary depending on the strength of the authentication protocol and method.

Strong Authentication

Today’s problems of identity theft and the misuse of identities and their attributes are accelerated by the ever-increasing amount of interconnected users, applications, and devices. To attain greater levels of authentication, identity management solutions require strong authentication. Over the last decade, strong authentication has been associated with both cryptography- and multi-factor-rooted authentication. Cryptography-based authentication means that the authentication protocol includes cryptographic operations in the identity and credential verification process. Table 2–4 on the following page provides descriptions of popular strong user and device authentication solutions.
Table 2–4
Overview of Strong User and Device Authentication Solutions

<table>
<thead>
<tr>
<th>Strong Authentication Solution</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strong User Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Hardware Tokens</td>
<td>Hardware tokens are liquid-crystal display (LCD) panel devices that display number sequences that change periodically, for example, once per minute. In combination with a PIN, the token’s software uses these sequences to create one-time passwords. Some tokens challenge the user with a built-in numeric keypad to calculate the passwords. Examples are the tokens from RSA (SecurID) and Vasco.</td>
</tr>
<tr>
<td>Smart Card–based Tokens</td>
<td>Smart cards are devices that can take a number of different physical forms. Most smart cards are similar to credit cards, with the addition of small, dime-size memory chips or microprocessors. USB tokens can operate similarly to smart cards, and some vendors have implemented smart card functionality on cell phones and PDAs. Smart cards and other tokens are tamper-resistant devices that can be used for secure storage of private keys, passwords, and other personal information. Some models perform private key operations (generation, signing, and decryption) in a safe, isolated manner on the card itself. Smart card solutions require smart card readers to be deployed or integrated with the devices.</td>
</tr>
<tr>
<td>Software Tokens</td>
<td>Software tokens operate like hardware tokens, except that a software program installed on a user’s workstation or other computing device (PDA or Pocket PC) provides a token generator or challenge/response system.</td>
</tr>
<tr>
<td>Biometric Authentication</td>
<td>Biometric authentication mechanisms match a physical characteristic of a user against a database record. Common methods include retinal, palm, or fingerprint scans, as well as voice authentication. After years of development, these systems are becoming more reliable, yielding fewer false positives and false negatives. Prices are also falling, making biometrics increasingly practical, though still far more expensive than free passwords. Biometric solutions are particularly successful in physical facilities authentication and government applications like border security and law enforcement.</td>
</tr>
<tr>
<td><strong>Strong Device Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Radio Frequency Identification (RFID)</td>
<td>An RFID system is a tag, which contains a miniscule computer chip and an antenna, that is attached to or embedded in an item. Items can be anything from a computer, to a dishwasher, to a living being. The tag transmits a signal to an electronic reader, which associates the signal with the specific item to which it is attached. The reader transmits this information to servers that collect and organize the data for tracking. RFID systems have the power to dramatically refashion such processes as the supply chain by making them more efficient, and they can bring direct consumer and societal benefits such as personalized shopping, medical reminders, and the identification of toxins before they reach landfills. However, the potential to tag and track every item raises privacy and civil liberty concerns. RFID technology has the potential to invade customer privacy and diminish customer control over personal information.</td>
</tr>
<tr>
<td>Trusted Platform Module (TPM)</td>
<td>A TPM, also known as a virtual smart card, is uniquely bound to a single computer platform and can be used for both user and device authentication. TPM core components are an RSA engine, a hash engine, a key generator, and a Random Number Generator (RNG).</td>
</tr>
</tbody>
</table>

**HP Strong Authentication Solutions**

HP offers a variety of strong authentication solutions. These include smart card technologies, biometric devices, RFID technologies, and TPM solutions.

HP ProtectTools Smart Card Security Manager is HP’s strong authentication solution rooted on smart cards. It has several unique features:

- Smart card in BIOS allows for pre-boot authentication and is OS independent.
- Smart card logon allows for strong, smart card-based Microsoft Windows authentication without requiring a PKI.

HP ProtectTools Smart Card Security Manager is available on several HP Compaq notebook models. For the current model list, see [www.hp.com/go/notebook](http://www.hp.com/go/notebook).

HP biometric solutions include the HP PCMCIA fingerprint reader and the HP built-in fingerprint reader for the HP iPAQ Pocket PC. For more information about current HP biometric solutions, see [www.hp.com/go/security/identity](http://www.hp.com/go/security/identity).

HP is leveraging its experience, expertise, and understanding of RFID technologies in its consulting services, and is one of the world’s largest players in the space. HP has taken a leadership role in developing RFID standards. In fact, HP was performing trials and pilot projects long before January 2005,
when Wal-Mart and the U.S. Department of Defense insisted that their suppliers begin using RFID tagging. With the world’s ninth largest non-military supply chain, HP wants to demonstrate the value of RFID systems for increasing the end-to-end speed and visibility of supply chains.

HP’s TPM solution is called HP ProtectTools Embedded Security. HP is the co-founder and leader of TPM specification development within the Trusted Computing Group (TCG). (For more information about the TCG, see www.trustedcomputinggroup.org.) HP ProtectTools Embedded Security is now available on many HP computers and notebooks. See www.hp.com/go/security/trusted for a complete list.

Single Sign-On

Single sign-on (SSO) is the ability of a user to authenticate once to a single authentication authority, obtain a credential token or artifact with a defined lifespan, and use it to access other protected resources without re-authenticating. The Open Group (www.opengroup.org) defines SSO as the “mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access permission, without the need to enter multiple passwords.”

HP and Single Sign-On

HP provides web-based SSO as part of HP OpenView Select Access, a web access-management solution. For enterprise SSO, HP takes a best-of-breed approach, leveraging the solutions from industry leaders such as Passlogix (v-Go SSO; www.passlogix.com) and Citrix Systems (Metaframe Password Manager; www.citrix.com). HP also offers HP ProtectTools Credential Manager, a client-side credential caching SSO solution in the HP ProtectTools suite.

Authentication Support in HP OpenView Select Access

HP OpenView Select Access is HP’s web access-management solution. The authentication methods it supports are presented in Table 2–5. Select Access supports at least three strong (two-factor and above) authentication mechanisms. These are: X.509 PKI certificates, RSA SecurID tokens, and Remote Authentication Dial-In User Service (RADIUS) tokens. HP also has considerable experience with building Select Access plug-ins to add support for other third-party strong authentication mechanisms and protocols.

Table 2–5
Select Access Supported Authentication Methods

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>User name/password as stored in the user’s Select Access Directory Server record</td>
</tr>
<tr>
<td>Microsoft Windows NT LAN Manager (NTLM)</td>
<td>Microsoft Windows domain authentication for authentication against Microsoft Windows NT, Microsoft Windows 2000, and Microsoft Windows XP domain controllers</td>
</tr>
<tr>
<td>Registration</td>
<td>Allows users to self-register to Select Access, resulting in a user record in the Select Access Directory Server</td>
</tr>
<tr>
<td>Security Assertions Markup Language (SAML)</td>
<td>XML standard allowing for the transfer of credentials (security assertions) between two authentication and authorization infrastructures, which allows controlled, trusted access between federated entities</td>
</tr>
<tr>
<td>Integrated Windows</td>
<td>Allows single sign-on to web-based applications through Microsoft Internet Explorer and Microsoft IIS from the desktop login, with no re-authentication required</td>
</tr>
<tr>
<td>SecureID</td>
<td>Support for RSA SecurID 2-factor token authentication</td>
</tr>
<tr>
<td>Remote Authentication Dial-In User Service (RADIUS)</td>
<td>Support for token solutions using the RADIUS challenge/response mechanism</td>
</tr>
<tr>
<td>Certificate</td>
<td>X.509 PKI certificate authentication using smart cards, cryptographic tokens, or certificates embedded in the browser, through client-side SSL authentication</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Support for authentication against Microsoft Windows 2000 domain controllers</td>
</tr>
</tbody>
</table>
The Select Access Policy Builder, a security policy management interface, allows for centralized administration of passwords and authentication policies. Password policy data is stored in the directory server. The Policy Builder supports two levels of password policy management: organization-wide policies and individual user preferences. Select Access provides the ability to define strong password policies, significantly increasing the security of password-based authentication.

Select Access supports native password management capabilities including password strength characteristics (length, detection of user name match, dictionary match, and password history), expiry policies, and account lockout based on suspicious behavior. Administrators can define expiration periods for users to change their passwords. They can also set temporary passwords for new accounts, forcing users to select a new password on first login.

**Authorization Technologies**

The goal of an authorization system is to protect resources and information while allowing fluid access for legitimate users of these resources. Authorization is the act of granting subjects access rights to protected resources. The main difficulty is scaling authorization policy administration to thousands—possibly millions—of subjects and protected resources. As the numbers grow, administrators need to reduce the ratio of policies to the number of subjects and protected resources without compromising the security of the system.

Authorization policies are rules for determining which subjects are allowed to access resources. In some cases, privacy considerations may require support for some form of anonymous or pseudonymous access. In most cases, however, users must be identified prior to receiving the authorization to access resources. An identity management infrastructure is therefore critical to establishing users’ identities as the basis for authorizing access to resources.

Two interesting access-control models used in the identity management infrastructure are the role based access control (RBAC) model and the rule set based access control (RSBAC) model. A role is an organizational job function with a clear definition of inherent responsibility and authority (permissions). The process by which an enterprise develops, applies, and maintains RBAC is known as role engineering. As old roles are retired or modified and new roles are defined to meet changing business needs, an enterprise defines processes for updating roles.

Role-based approaches are suitable when job functions are easily partitioned. Wide-scale implementations remain stalled because of the complex nature and large scope of role engineering projects, transitory job assignments in knowledge-based organizations, lack of funding, limited standardization, and proprietary access control mechanisms. A common challenge facing role-based systems is finding agreement among stakeholders for standardized vocabularies and role definitions.

An alternative to an RBAC approach is RSBAC. Most web access-management products adopt RSBAC, including HP OpenView Select Access. With this approach, access is granted or denied based on a set of pre-defined rules or organizational policies. Access control decisions can change dynamically based on access control policies. Rules are context dependent: they can take into account things like the time of day, resource type, and access location.

**Authorization Support in HP OpenView Select Access**

Web access-management products like HP OpenView Select Access typically combine basic RBAC support (with limited hierarchy and constraint capabilities) and RSBAC support.

With its matrix-based representation of users and resources, HP OpenView Select Access Policy Builder simplifies the complicated and often time-consuming process of creating and applying authorization policies. With simple visual icons and inheritance rules, the Policy Builder makes policy logic easy to
understand. This reduces the amount of errors typically incurred by other list-based access management systems. Beyond simple allow and deny authorization policies attached to each matrix intersection, the Policy Builder allows for further control with conditional access rules.

Auditing Technologies

Auditing systems capture security-related events in identity management systems and ensure accountability for the underlying IT and security infrastructure. Complete and accurate audit and event records provide the evidence that enterprises need to demonstrate compliance with business, security, legal, and regulatory mandates. It is especially critical to audit the authorization, provisioning, and privacy components of identity management systems, which may create or remove user privileges and accounts.

HP OpenView Select Access Secure Audit Server

The HP OpenView Select Access Secure Audit Server provides a consolidated security logging and audit trail. All access requests, authorization decisions, and administrative changes are logged and can be digitally signed to prevent tampering of audit data.

The Secure Audit Server outputs to multiple destinations including databases, e-mail messages, UNIX® syslogs, Microsoft Windows Event Logs, and files. Different output destinations can be configured based on the type of audit data, such as audit component and event level (for example, information and warning). All components can store logs and audit information locally in addition to forwarding them to centralized secure audit servers or databases.

HP Select Access by default gathers audit information within all its server components and policy enforcer plug-ins located on the web/application server platforms. This information is a complete record of all transactions within a given Select Access component. Select Access natively stores audit logs and system logs in an ASCII text file using an XML format.

The Secure Audit Server can log information centrally or forward it to any of the supported repositories. It can also make this information tamper-proof by applying digital signatures to the audit trail. Customers have utilized this technique to consolidate audit information from a number of sources.

A Report Viewer interprets the output log files and audit databases collected by the Secure Audit Server. HP Select Access Secure Audit Servers can also send audit information alerts via e-mail to administrators. This can be tied into Simple Network Management Protocol (SNMP) tools through e-mail to SNMP gateways.

Privacy Management

In the context of electronic privacy, users express concerns regarding today’s IT systems and environments like the Internet. Some of the key privacy concerns include:

- Data is collected silently. This is facilitated by the web, which allows large quantities of data to be collected inexpensively and unobtrusively.
- Data from multiple sources may be merged. Non-identifiable information can become identifiable when merged with other sources and information.
- Data collected for business purposes may be used in civil and criminal proceedings.
- Data collected for business purposes may be forwarded to third parties, without notifying the user.
- Users are not given meaningful choices for the use of their personal data.
Privacy considerations typically arise when an organization needs to collect and store customer, employee, and other private data. Other situations that raise privacy concerns include demonstrating conformance with privacy regulations and forwarding user information (identity information, web-service access information, security assertions, or localization data) to third-party service providers.

Numerous efforts have produced legislative frameworks for privacy. Examples are the EU Directive on Data Protection, U.S. laws such as HIPAA and the Children’s Online Privacy Protection Act (COPPA), and frameworks such as Safe Harbor. However, privacy and data protection laws are hard to enforce when personal information spreads across boundaries. In general, users have little understanding or knowledge of privacy laws and their implications. For additional information, see www.privacyinternational.org/survey/phr2003.

Privacy management in an IT environment has many different aspects. These include negotiation, policy life cycle management, enforcement, monitoring, decision support, violation detection, preserving computation, data minimization and transformation, rating and branding, verification and certification, auditing and accountability, mediation and delegation, anonymization and pseudonymization, and user training. In the context of identity management solutions, privacy-protecting technologies can be viewed as an extension to authorization systems. Authorization policies control data access based on factors like privacy regulations and user consent.

Privacy management is an identity management area that requires much work and effort. HP and other major IT players like IBM are leading key developments in the privacy management space. HP is involved in several cross-industry and government-driven privacy standardization initiatives.

"Privacy isn’t just about hiding things. It’s about self-possession, autonomy, and integrity. As we move into the computerized world of the twenty-first century, privacy will be one of our most important civil rights. . . It’s the right of people to control what details about their lives stay inside their own houses and what leaks to the outside."

—Simson Garfinkel, Database Nation
Identity Life Cycle Management

Provisioning solutions are similar to SSO solutions in that they operate from the top down; the application manages all of the systems under it. Administrative functions—from the essential add, modify, and delete to the more general maintenance and monitoring—are under the control of the provisioning system. Provisioning functions can also include non-electronic tasks such as identifying a cubicle, connecting a network port, and acquiring a PC.

With provisioning products, organizations risk implementing one solution that can potentially clash with another. Provisioning solutions often incorporate other parts of the identity management framework, such as self-service and password management.

The only mature provisioning-specific standard at this time is the Service Provisioning Markup Language (SPML). SPML messages facilitate the creation, modification, activation, suspension, enablement, and deletion of identity-related data in different identity repositories. The Organization for the Advancement of Structured Information Standards (OASIS) has been working on the SPML specification since late 2001. For more information, see www.oasis-open.org/home/index.php.

HP OpenView Select Identity

HP OpenView Select Identity is a scalable solution for managing identity within and between large enterprises. The Select Identity solution automates the process of provisioning, managing, and terminating user accounts and access privileges across platforms, applications, and corporate boundaries.

The key features of the Select Identity system include:

- **Business-process aligned management** easily and rapidly manages business or technology changes at micro or macro levels within the managed environment.
- **Centralized management** provides a single point of control for the management of users and entitlements.
- **Provisioning** automates creating, updating, and deleting accounts and entitlements on information systems across the enterprise.
- **Administrative delegation** enables administrative rights to be distributed among multiple tiers of functional departments, customers, and partners.
- **User self-service** enables end users to initiate access to services, change passwords, set password hints, and update general identity information through a simple web browser interface.
- **Approval workflow** automates approval processes required for granting access privileges to users.
- **Password and profile management** manages and distributes password and user profile information across and between enterprise information systems.
- **Auditing and reporting** provides standardized reporting on actions and user account activity.
- **Fully scalable and resilient operation** facilitates today’s global, 24x7 businesses.

Select Identity Architecture

Select Identity is an event-driven, Java 2 Enterprise Edition (J2EE) application that enables clustering, failover, multi-phase commit, and asynchronous operation. All requests to and from the system use HTTP.

Leveraging an open-standard, J2EE Connector Architecture (JCA) bus, Select Identity uses predefined connectors to access backend system data stores. Custom connectors can be readily created, and Select Identity offers a software development kit (SDK) for this purpose. For an up-to-date list of the currently supported connectors, see www.openview.hp.com.
Identity Management With Select Access and Select Identity

Together, Select Access and Select Identity provide a complete answer to complex organizational identity management needs:

• Complete user provisioning for internal and external users
• Easy to manage access and authorization for complex business rules
• Identity life-cycle management, to ensure no lost or forgotten users
• Full-featured user self-service, which cuts the costs of administration
• Multi-step approval workflow ensures the correct authorities are granted
• Profile and password synchronization simplify the user experience
• Password management and self-reset make it easier for users and call desks
• Business process modeling matches the business need
• Full delegated authority provides control where it should be
• Single sign-on aids staff productivity
• Account terminations ensure effective security
• Audit and reporting ensure demonstrable compliance

Federated Identity Management

Federation enables the trusted interchange of security-related information between different autonomous policy domains. Security-related information includes authentication, authorization, and auditing data. Although federation is generally used in the context of an inter-enterprise security mechanism, it can also be used within an enterprise to provide tighter integration between loosely coupled ecosystems.

Typically, a federation provides a common framework for trust—a standard syntax, vocabulary, attribute set, and set of policies and practices for the trusted interchange of security-related information. Bilateral (federation) agreements between partners are often required to negotiate the specifics of access, such as which users or systems can access which resources, under what circumstances, and under what contractual relationships. Access control always remains with the owner of the resource. A federation might also define minimum acceptable trust levels or authentication mechanisms required for specific circumstances.

A federation agreement always deals with two entities: an asserting party that generates security assertions and a relying party that trusts the security assertion made by the asserting party. There are a number of federations being formed, supporting a variety of vertical marketplaces, communities of interest (financial services, health sciences, research and education), and geo-political boundaries (state and national governments).

A variety of standards, specifications, and protocols relate to federated identity management. Figure 2–5 shows the positioning of some of the relevant federated identity management standards. The Liberty Alliance specifications define the protocol messages, profiles, and processing rules for identity federation and management. They rely heavily on other standards such as SAML and WS-Security. Additionally, the Liberty Alliance has contributed portions of its specification to the technical committee working on SAML. More information is available from www.projectliberty.org. HP endorses the Liberty Alliance and actively participates in the creation of its specifications.
SAML is an OASIS specification that provides a set of XML and Simple Object Application Protocol (SOAP)-based services, protocols, and formats for exchanging authentication and authorization information. Currently, work is under way for SAML version 2.0. More information is available from www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

WS-Security is another OASIS specification that defines mechanisms implemented in SOAP headers. These mechanisms are designed to enhance SOAP messaging by providing a quality of protection through message integrity, message confidentiality, and single message authentication. More information is available from https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.


Other identity management enabling standards are:

- XML Key Management Specification (XKMS), www.xmltrustcenter.org/xkms/index.htm
- XML Signature, www.w3.org/Signature
- XML Encryption, www.w3.org/Encryption

HP and Federation

HP OpenView Select Federation allows secure and quick extension of enterprises to business partners by enabling rapid integration between different identity systems within and across corporate boundaries. Using industry standard federation protocols, Select Federation links multiple accounts with different providers on the Internet so that secure authentication occurs once per session. Select Federation also enables service providers to offer secure, mobile federated identity services for sharing distributed identity information while protecting the privacy of service consumers.

HP OpenView Select Federation is a protocol-neutral and vendor-neutral solution. It currently supports the Liberty Alliance and SAML protocols, and it will support the WS-Federation protocols when they are ratified. It can also integrate with any vendor’s identity management solution, allowing organizations to protect their investment without worrying about which protocol or vendor to choose for the future.

Select Federation currently supports the following federation protocols:

- SAML 1.0 and SAML 1.1
- Liberty ID-WSF (Liberty Alliance Certified Interoperable)
- Liberty ID-PP (Personal Profile Service)
- Liberty ID-EP (Employee Profile Service)
- Liberty ID-FF 1.2 (Liberty Alliance Certified Interoperable)
- Liberty ID-FF 1.1 (Liberty Alliance Certified Interoperable)
- Liberty LECP (Liberty Alliance Certified Interoperable)
- WS-Security

Identity Management Summary

Identity management is the ability to identify every user, application, or device across organizations and provide flexible authentication, access control, and auditing while respecting privacy and regulatory controls. Delivered via a set of processes and tools for creating, maintaining, and terminating a digital identity, these tools allow administrators to manage large populations of users, applications, and systems quickly and easily. They allow selective assignment of roles and privileges, making it easier to comply with regulatory controls and contribute to privacy-sensitive access controls.

For HP, identity management is centered on the pervasiveness of identity management technologies and solutions:

- Identity management is about the management of user, application, and device identities.
- Identity management is about the management of identities in different contexts: enterprises, SMBs, and consumers.
- Identity management deals with the management of the entire life cycle of identities and their attributes.

<table>
<thead>
<tr>
<th>Solution</th>
<th>IDM Focus Area</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP ProtectTools Smart Card Security Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP OpenView Select Access</td>
<td>Web access management and web single sign-on</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP OpenView Select Identity</td>
<td>Identity provisioning</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP OpenView Select Federation</td>
<td>Federation</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP Identity Management Services</td>
<td>IDM Consulting and Integration, IDM Managed Service</td>
<td><a href="http://www.hp.com/go/security">www.hp.com/go/security</a> Click Security Services (under Featured Products and Services)</td>
</tr>
</tbody>
</table>