
5 Identity and Access Management (IAM)

Rudolf Wildgruber

5.1 Challenges

Today's business environment is a challenging one for identity and access management in the enterprise. Business relationships are growing more complex, blurring the line between internal and external business processes. They are also more dynamic, requiring greater flexibility and responsiveness in the enterprise's business practices, policies and processes. Companies are under pressure to open up their IT infrastructure to an ever-increasing number of users, both inside and outside the company and to ensure the highest productivity and privacy for these users, all while controlling IT administrative costs and leveraging existing investments wherever possible. Now more than ever, granting the right people the right access to the right resources at the right time is an essential element of enterprise security as companies strive to protect their corporate data and systems and remain innovative, productive, responsive, compliant and cost-effective business entities.

In the conventional IT infrastructure used in most big companies today, there is a one-to-one correspondence between a function or resource available to users and the IT application/system that provides that function. Consequently, user management, access management, password management and auditing are carried out on a per-IT system basis. IT staff must administer users and their access rights on each IT system in the network, usually by manual administration. Users get one account and one password for each IT system they need to use. Each IT system has its own audit or monitoring function to track changes to users and their access rights on that system.

This structure has negative consequences for identity and access management:

- Decentralized user management and provisioning means that identity and access data is duplicated across IT systems and usually becomes inconsistent over time, making it difficult to find correct and up-to-date information and to de-provision users.
- One password per IT application means that users must remember a lot of different passwords, one for each system they need to use. Password proliferation leads to more help desk and hotline calls, lost productivity as users wait for password resets and increased IT administration costs.
- Manual administration is expensive and leads to delays in provisioning and de-provisioning users, which decreases productivity, jeopardizes security and leads to data inconsistencies.

- Decentralized auditing and monitoring makes it difficult to track changes to users and their access rights. There is no way to tell what a single user's total access rights are across the enterprise, making it difficult to audit for regulatory purposes.

Overcoming the present limitations requires an enterprise-wide, cross-platform, centralized and automated user management, provisioning and access management system, which controls access to IT resources based on business roles, policies and processes. The system must provide ways to align itself with business processes and off-load routine administrative functions and decisions from IT staff to users and their managers so that decisions about what users really need are made by the people who know best. Identity and access management (IAM) technology has evolved to a well-defined market category and has reached the depth and breadth to offer an effective way to satisfy these requirements.

5.2 Use Cases

Identity and access management (IAM) is an integrated solution that makes user and access management transparent across the different systems that make up the enterprise's IT infrastructure. The Burton Group defines IAM as “the services, technologies, products and standards that enable the use of digital identities”. *Identity management* addresses the need to administer users and security policies across the IT infrastructure, while *access management* addresses the real-time enforcement of the security policies in force for each user of the enterprise IT infrastructure. A *directory server* is most commonly used as the data repository for identity and access management solutions.

Here are some real-life scenarios that illustrate how IAM works.

5.2.1 Making a New Employee Productive Quickly

Figure 5.1 illustrates how the IAM system works when a new employee is hired:

- The personnel department enters the master data for the new employee into the human resources (HR) system and the master data is automatically synchronized with the IAM system's identity store.
- The IAM system automatically assigns the appropriate privileges to the employee based on the rule-based security policies (called provisioning rules) established and saved in the identity store.
- An identity administrator optionally assigns individual privileges to the employee.
- According to the employee's privileges, the IAM system automatically determines the IT systems that the employee needs to have access to and the access rights for these systems.
- The IAM provisioning system automatically generates accounts in the IT systems and sets the access rights. For example, the IAM system generates an account for Intranet and Extranet access, a mailbox as well as accounts for other enterprise IT systems.

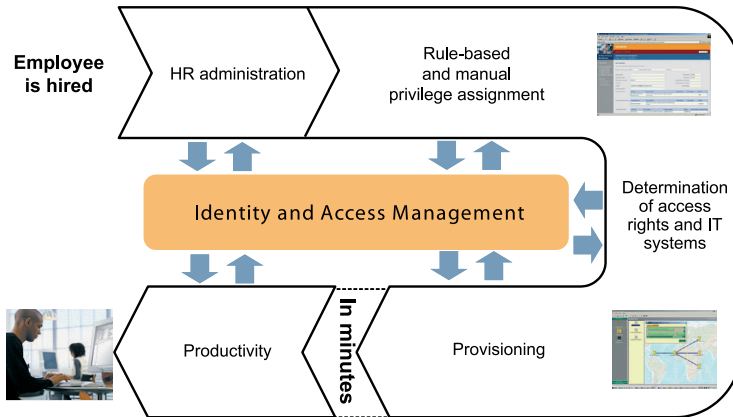


Figure 5.1 Making a new employee productive quickly

- The IAM provisioning system also sets the employee’s access rights in the central web access management system for the portals s/he will use.

The new employee has now access to the relevant IT systems with the access rights defined in the privileges assigned to him/her.

5.2.2 Changing an Employee’s Job Function

In this use case, an employee is switching from the Sales department to the Marketing department effective February 1st. S/he is currently authorized to perform sales activities in the sales portal, but will need to use the marketing portal as of February 1st. The IAM system handles the required access rights changes as follows (see Figure 5.2).

- The personnel department enters the change in department into the HR system and the change is synchronized with the IAM system via a “department” user attribute.

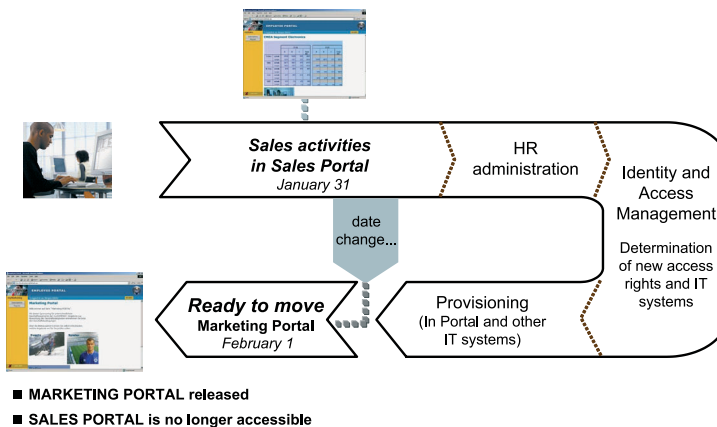


Figure 5.2 Changing an employee’s job function

- The IAM system records the departmental change in the entry for the employee in the identity store (in the “department” user attribute) and automatically determines the employee’s access rights based on the new value.
- The IAM system revokes the access rights associated with the privilege “Sales”.
- The IAM provisions the access rights associated with the “Marketing” privilege.
- The Marketing portal is made available to the employee and the Sales portal is no longer accessible to the employee.

5.2.3 Changing a User Password

Figure 5.3 illustrates what happens in the IAM system when a password that can be used for several applications is changed:

- A user changes his/her password on first logging in to a Windows system.
- The IAM system discovers the password change and saves it in the entry for the employee in the identity store.
- The IAM system synchronizes the changed password on the employee portal.
- The changed password is available to authenticate against the employee portal.

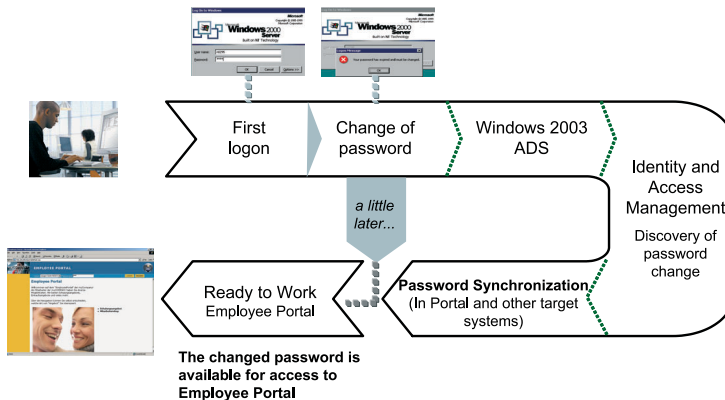


Figure 5.3 Changing a user password

5.2.4 Authorizing an Order

In this use case, a sales employee needs access to an analyst report and this access must be authorized. The IAM system handles this case using a request workflow (see Figure 5.4).

- The sales employee orders the report.
- The IAM system runs a request workflow that handles the authorization process and automatically forwards the request to Sales management.
- Once Sales management has authorized the request, the IAM system provisions the changes in access rights in the Sales portal.

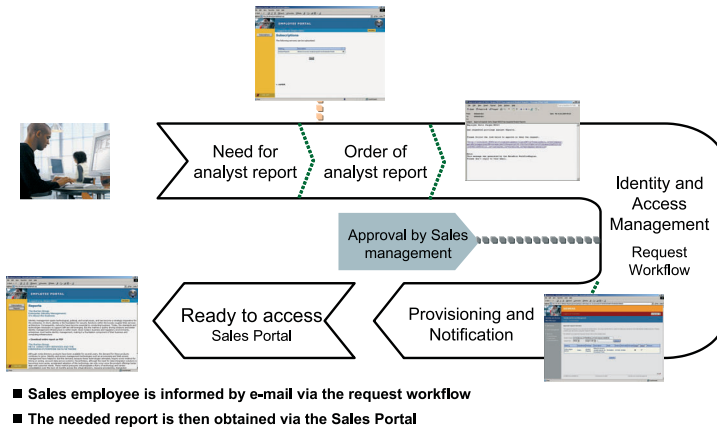


Figure 5.4 Authorizing an order

- The IAM system informs the Sales employee via e-mail that access to the analyst report has been granted.
- The employee then obtains the analyst report from the Sales portal.

5.2.5 Web Single Sign-On

In this use case, sales employee Mr. Maier wants to generate his monthly order income report, enter a new customer contact and report recent travel expenses. The IAM systems support these tasks with web single sign-on (see Figure 5.5).

- The sales employee Mr. Maier accesses the employee portal.
- The employee portal requests Mr. Maier to authenticate with user name and password. The web access management system creates a session for Mr. Maier.
- Mr. Maier opens the order income application. The web access management system grants access and supplies the session information to the order income application in the background. Mr. Maier fills in the report parameters and generates the report.

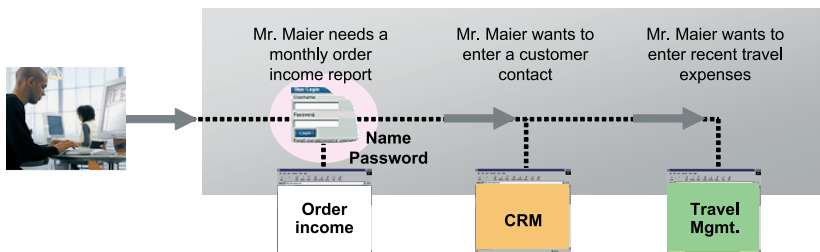


Figure 5.5 One-step authentication for accessing multiple applications

- Mr. Maier now opens the CRM application. The web access management system grants access and supplies the session information to the application in the background. Mr. Maier creates a new customer record.
- Mr. Maier now opens the travel management application. The web access management system grants access and supplies the session information to the application in the background. Mr. Maier enters travel details and costs.

Mr. Maier had to authenticate only once to have access to multiple applications. The web access management system made authorization decisions when Mr. Maier tried to open the applications and granted access according to central security policies.

5.3 Components

5.3.1 Directory Services

Directory services are critical components of today's highly interconnected business environment. Directory services provide the foundation for identity and access management across the ever-widening boundaries of the enterprise:

- In the Intranet environment, the directory service provides a global repository for shared information about employees, organizations and resources such as applications, network devices and other distributed services, accommodating hundreds of thousands of users.
- In the Extranet environment, the directory service maintains profile information about customers, trading partners and suppliers, accommodating millions of users.

For both these environments, the directory service must be able to manage user identities and control access to the information and services offered to its users, and it must provide fast, constantly available, authenticated access to the information and services, potentially to a vast number of users. The ideal directory service for today's enterprise:

- Integrates the disparate service- and platform-specific databases, profiles, policies and provisioning processes within the enterprise's infrastructure into a centralized service- and platform-independent model that is always up to date
- Supports advanced, complex identity management services to guarantee data security
- Provides the performance and scalability required to manage user identities and control access to information and services by potentially tens of millions of users.

Directory services are often complemented by virtual directories or LDAP proxies.

A virtual directory is a middleware solution, acting between directory-enabled clients on one side and database systems or multiple directory servers on the other side. The virtual directory appears as a single directory server to the client. Internally the data is collected from distributed sources and technologies but presented as having originated

from one source. To retrieve data from database systems, the virtual directory translates directory queries and commands into SQL statements for read/write operations. Like an LDAP proxy, a virtual directory is not a repository and does not have a persistent store. Virtual directories are used in environments where

- Identity data that is stored in multiple repositories needs to be merged on-the-fly
- The application data format needs to be reconciled with the infrastructure format.

An *LDAP proxy* is a directory server front-end that simply redirects directory requests to other directory servers. An LDAP proxy is often used for load balancing or to provide a single point of access to multiple directory servers. In contrast to a virtual directory, an LDAP proxy redirects a single directory request to only one directory server and does not merge data from multiple sources.

5.3.2 Identity Management

The **process** of identity management includes identity creation and clearing, privilege assignment, provisioning and auditing.

Identity Creation and Clearing. The first step in the identity management process is to create a unique digital identity for every user of the enterprise IT systems. Information about users is usually managed in authoritative systems like HR systems (employees), CRM systems (customers and partners) and SCM systems (suppliers). The IAM system imports the user information from the authoritative sources into a central repository where all the privileges of the users are maintained during the life-cycle of the user. Importing of user information goes along with consolidation of user data, like normalizing or correcting misspelled certain user attributes. The creation of a unique user ID and the synchronization of that ID with the source systems help to keep the user information consistent in all connected systems. For example, if a user changes his/her surname as a result of marriage, the unique user ID allows the related user information to be found in the central IAM repository and the name change to be adopted from the source system.

Privilege Assignment. In an IAM system access rights to IT systems are established based on privileges. Therefore, the next step in the identity management process is to assign one or more privileges to users. Provisioning rules can be used for automated privilege assignment. The rule-based provisioning model works well when access rights depend on the values of user attributes – like a departmental or managerial function. Thus, a change in a user attribute value triggers an immediate de-provisioning and reprovisioning. Manual assignments of privileges are necessary when access rights are more static – when they depend on the person’s job, for example, educational services trainer or quality manager. In this case, privileges don’t need to change when organizational attributes change. In reality, rule-based assignment is often combined with manual assignment.

Provisioning. Provisioning is the dynamic process of establishing the target system-specific access rights to which a user-to-privilege assignment ultimately resolves. Provisioning is a two-step process:

1. Calculating the accounts, the groups, the target systems to which the groups belong and the account group memberships that result from the privilege assignments to users and creating the account, group and group membership data in the identity store – this process is called privilege resolution and can involve the matching of user attributes to provisioning policies, permission parameters or role parameters to determine the appropriate groups and target systems.
2. Synchronizing the access rights data in the identity store with the target systems – this process physically transfers the access rights data from the identity store to the target systems.

Auditing. The identity audit collects information on all user and privilege management actions; for example a change in a user's data that affects a privilege assignment. Auditing functions include writing audit records for access requests and decisions, evaluating these audit records and generating reports. The audit ensures that the activities associated with identity management are logged for day-to-day monitoring to prove regulatory compliance and for corporate knowledge purposes.

The main **services** of identity management include user self-service and delegated administration, password management, user management, privilege and policy management, request workflow, provisioning and metadirectory.

User Self-Service and Delegated Administration. *User self-service* allows users to perform simple user-oriented identity management tasks that must typically be carried out by technical IT administrators in the traditional enterprise IT infrastructure. With self-service, users can manage their own data, including their own passwords and request privileges – user access rights to resources in the IT systems in the enterprise network – for themselves.

Delegated administration allows users to delegate their identity management tasks (or a subset of these tasks) to other users. Delegation allows an enterprise to distribute identity management tasks according to business functions and to create a hierarchy for identity management that reflects its business structure.

Together, self-service and delegated administration permit the enterprise to balance the user management and access rights administration load across the enterprise and to off-load identity management tasks from IT, hotline and help desk staff to the people who really need to be able to perform them.

Password Management. Password management allows users to maintain a single password that will automatically be synchronized with all relevant IT systems in the enterprise. Password management functions allow users to change and reset their passwords in one or more systems – for example in an LDAP directory or in Windows, notify users when they need to change their passwords to comply with password policies established for the enterprise (for example expiry of a password's lifetime) and synchronize these password changes in real time to all the relevant IT systems. Forgotten passwords can be reset by the user through a challenge-response procedure, or by an administrator.

User Management. User management includes all activities related to the creation, maintenance and use of user accounts, user attributes, privileges, etc., encompassing the different directories, user databases and application-specific repositories that make up the fragmented, heterogeneous enterprise IT environment. User management consists of two main tasks: maintaining an accurate and up-to-date directory of users to be provisioned and assigning users to privileges. The task of maintaining a consistent user directory is handled by request processes from the users themselves and/or their managers (user self-service and delegated administration) and by data synchronization workflows (e.g. with the enterprise HR system) provided by the metadirectory.

Privilege and Policy Management. A *privilege* is a set of access rights based on either business semantics or on IT system specific semantics that permits users to access enterprise IT resources. The enterprise can structure its privileges in a hierarchical model according to its business roles and functions or based on other considerations. Privilege management establishes a logical layer for the modeling and management of authorization (access control) information that is generic enough to cover many of the relevant IT system's authorization/access control methods:

- Group-based IT systems control access rights via account membership in groups. Making an account a member of a group gives the account the access rights that have been granted to the group. User groups, profiles, and application-specific roles are examples of group-based methods of access control.
- Attribute-based IT systems control access rights via attributes in the accounts. For example, in Active Directory, a set of account attributes defines a user's mailbox; there is no concept of group membership.
- Some systems, like Microsoft Active Directory, provide both types of access control.

Privilege-based access management allows managing access control on each IT system in a uniform way. Privilege management also simplifies and structures access rights administration. High-level managers can assign privileges to their staff without needing to know the lower-level details, and IT personnel can administer the access rights in the IT systems without needing to know the higher-level details.

Policy Management comprises the management of security and administrative policies. Policies are composed of one or more rules and each rule defines the objects subjected to the rule (e. g. a set of users), the action to be performed and a priority to handle conflicts with other rules properly. Administrators define rules for consolidation of user data, privilege assignment, reconciliation and audit to determine how the identities and their access rights will be managed.

Request Workflow. Request workflows allow users to request privileges, which in turn must be authorized by various approvers according to the security policies in force in the enterprise. Administrators set up an approval path based on business policies; the workflow then notifies each person in the path – for example, by e-mail – that s/he has an approval request to handle. The approver uses a web browser to access a web interface to grant or deny the request.

Provisioning. Provisioning is the fully automated process of calculating user access rights and distributing them to IT systems based on the privileges assigned to the user. The provisioning process automatically grants, changes and revokes access rights in IT systems in response to privilege assignment, re-assignment and revocation.

Provisioning automates the time-consuming process of managing access rights across many different IT systems over the user life-cycle and permits fast activation and de-activation of access rights across these systems for multiple user identities.

Provisioning provides a single point of administration for the enterprise's total identity and access control information and implements the services that keep the identity and access control data in the IT systems consistent and up-to-date, allowing the enterprise to ensure the security of its data, reduce administration overhead, accelerate its business processes and improve its customer service as well as protect its investments in existing IT systems.

The validation of IT systems is a periodic comparison between the account and group data in the IT system and the central IAM repository. Validation is necessary to check for and detect local changes to the IT system data that have occurred independently of changes initiated by the IAM system. Deviations are reconciled either manually or automated through rules.

Metadirectory. Metadirectory is the set of services that integrates the disparate directories, user databases and application-specific information repositories in the enterprise IT network into a centralized data store and provides the connectivity, management and interoperability functions that unify the user data ("join") and ensure the bidirectional attribute flow (synchronization) in this fragmented environment.

In an IAM system, the metadirectory provides an infrastructure for automated enterprise-wide user management that addresses the problem of decentralized multiple user identities and user administration functions. Metadirectory services:

- Integrate user data from multiple authoritative sources – human resources directories, enterprise resource planning (ERP) systems, customer relation management (CRM) and supply chain management (SCM) databases – into a single, unique digital *identity* that represents the user to be provisioned in the IT systems
- Maintain an accurate and up-to-date *identity store* of these identities and synchronize identity data from the identity store back into the authoritative sources.

5.3.3 Access Management

The **process** of access management includes authentication, authorization and audit.

Authentication. Authentication is the step of identifying users and verifying their identity. Various authentication methods can be used, including basic or form-based authentication using username/password, secure tokens, digital certificates and smart cards. Authentication ensures that authorization is performed for the identified user who accesses enterprise resources.

Authorization. Authorization is the real-time enforcement of user access requests to the enterprise IT systems and resources. When a user tries to access a resource, a decision is made if the access is granted or denied. Access decisions are usually based on security policies. Authorization ensures that users can only access enterprise resources according to the policies in force.

Audit. Audit in access management collects information from all enforcement points in the access management process and evaluates and reports this information. Auditing functions include writing audit records for access requests and decisions, evaluating these audit records and generating reports. Audit ensures that the activities associated with access management are logged for day-to-day monitoring, to prove regulatory compliance and for corporate knowledge purposes.

Information can be provided about:

- Which tasks have been performed by an administrator
- Which operation has been performed by an identity
- Which events have occurred
- Which specific operations have been performed successfully or unsuccessfully.

The main **services** of access management include authentication, authorization, audit as described above and policy management, web single sign-on, enterprise single sign-on, federation, web services security, auditing and reporting.

Policy Management. Policy Management is the administration of the security policies. Policies are composed of one or more rules and each rule implements part of the policy. Administrators define authentication, authorization and audit rules to determine how the applications and resources will be protected and managed.

Web Single Sign-On. Web Single Sign-on (Web SSO) gives every user a one-step authentication for access to multiple web resources or applications. Having authenticated a user, Web SSO creates a single sign-on session using an encrypted cookie to store user authentication and session information. The user is freed from the need to authenticate multiple times.

Enterprise Single Sign-on. Enterprise single sign-on is the enlargement of single sign-on to non-web resources. This typically comprises host and terminal as well as database and application-specific authentication. To achieve this functionality, the client needs SSO-specific software, which takes care of the login procedures for these enterprise applications.

Federation. Identity federation permits an enterprise to share trusted identities with autonomous organizations outside of the enterprise, like trading partners or suppliers. The goal of federation is to integrate identity information across enterprise boundaries to allow the enterprise to build business communities.

Web Services Security. To allow business integration with partners, customers and suppliers, applications expose service-oriented interfaces, commonly known as web services. Web services security deals with securing the web services based integration of applications across enterprise boundaries. Specifically, web services security allows

access to the services to be controlled, the service level and quality of service agreements to be enforced and monitored and the source of failures to be diagnosed.

Reporting. Reporting in contrast to audit and logging is used to retrieve static information about data in the repository. It can be viewed as an extended view of certain objects or attributes.

5.4 IAM for Heterogeneous Environments

An IAM solution provides uniform and business-oriented management of identities and enforcement of access control, especially in situations where a heterogeneous IT and application infrastructure exists. The focus here is on supporting a large variety of systems and applications, for example

- Platforms like Windows, Linux and Unix
- Applications like SAP R/3, mySAP ERP, SAP NetWeaver, Siebel, Peoplesoft
- Databases like Oracle, MS SQL, IBM DB2 and
- Others like communication systems and content management systems.

Figure 5.6 shows a typical scenario in a heterogeneous environment.

- Portals are already in widespread use as cross-domain, process-oriented interfaces. Whether as employee portals for access to internal applications, partner or supplier portals for collaboration along the supply chain, or customer portals to improve customer relationships – portals are always the interface to a series of applications.
- Internal and external users have access to the applications through the portal. Access management authenticates all access via the portal centrally and enables single sign-on. Access management then controls which user is allowed to access

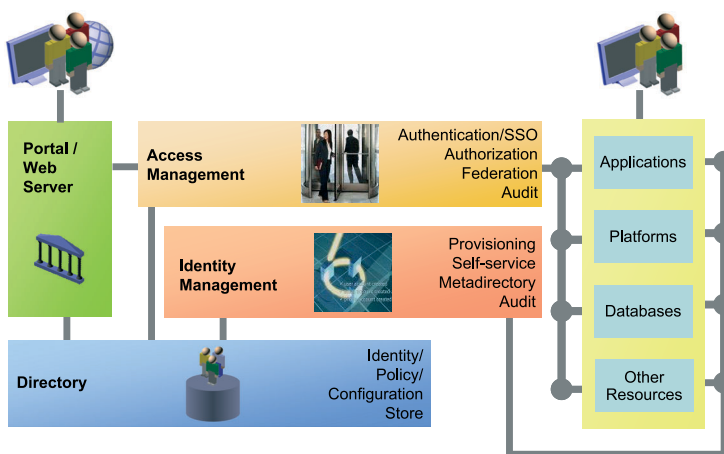


Figure 5.6 Identity and access management in a heterogeneous environment

which application and how by means of guidelines, policies and rules. A directory service stores identity, policy and configuration data.

- Identity management centrally manages all internal and external users and their privileges. The portal and all applications are provisioned with user accounts and access permissions. By assigning cross-platform privileges the identities are granted access rights in the portal and all applications in one step. In addition to using a portal, internal users can access applications directly from their desktops.

5.5 IAM and Regulatory Compliance

An often underestimated problem in connection with identity and access management is compliance, i.e. the clear and demonstrable observation of legal regulations. The debate here is currently centering on US standards such as HIPAA in the health sector or the Sarbanes-Oxley Act (SOX) for accounting (see Chapter 1). These are also of importance for many European enterprises.

However, one point that is overlooked is that European and German regulations, such as KonTraG (Corporate Control and Transparency Act), BDSG (German Data Protection Act), the European Data Protection Directive, as well as regulations on risk management in the German Law on Limited Liability Companies and Stock Corporation Law and the strict guidelines on risk management under Basel II, form a closely meshed network of compliance requirements.

An IAM solution can ensure that an enterprise does not become entangled in this web. This is because a consistent view of “who” is necessary to ensure that the question “Who is allowed to do what where and who did what where?” can be answered. If an employee has different digital identities in a number of systems, it is difficult to obtain a complete overview of the authorizations assigned to the employee and his or her compliance-related actions. The IAM solution can ensure that defined and stringent processes for managing identities and access permissions are implemented. Users must not be created and given access authorizations in an ad hoc fashion. Every change to user information and every assignment of rights must be structured and documented. Internal IT processes are optimized and standardized by means of self-service functions, delegated administration and request workflows. The creation of users in different systems and their assignment to roles and groups is controlled centrally and always carried out in the same way. Access decisions can be controlled and monitored centrally. Together with the auditing and reporting services in an IAM solution, this creates the foundation for compliance.

5.6 Conclusion

Enterprises and other organizations need to be able to identify everyone involved in their business processes – unambiguously. They have to control which persons with which rights can access which resources and when.

Information about users is typically stored in numerous distributed directories, while the applications and services to be protected are based on heterogeneous platforms. In such a situation, ensuring compliance with legal requirements is a very complex task. If communication security policies and compliance requirements are to be enforced permanently and throughout an enterprise, all directories must first be kept up-to-date and consistent – on the fly. Secondly, it must be possible to update the user authorization profiles for all systems from a central point of administration and across all platforms. These two requirements can only be met by comprehensive identity and access management that provides user data centrally, grants permissions dynamically – and controls access securely.

Identity and access management also opens up new possibilities for strategic partnerships. Joint and trusted use can be made of identities with partners outside the enterprise network (federated identities). Users can easily switch between the partner's domains and applications without having to sign on again.