

IDM DEFINED

Iana Bohmer
Commercial Service
Northrop Grumman IT

IDM DEFINED

The term “Identity Management” is a general term that has different meanings depending on the audience, but they all relate to the fundamental concept of a process or system that collects, verifies, stores, and recalls representations of a person’s identity for the purposes of authentication for granting entry into an organization’s facilities and resources. (Although IDM typically refers to identification of individuals, it also can be applied to objects.) IDM applications refer to systems that search and track identification data concerning an individual such as criminal and medical histories for the purpose of creating a current profile. The following processes all are considered aspects of IDM: identity proofing, identity profiling, identification card/badge issuance, physical access systems, biometrics authentication, PKI scheme for logical access, password issuance and management, password synchronization, digital signatures, directory services, Web single-sign on, provisioning (assigning access rights based on organizational roles), and federated identities, to name a few.

IDM is a term that covers products, software, applications and processes from authentication to access management as well as the infrastructure that supports them. However, the critical link is between the technology and business process. Enterprises must facilitate a rational relationship between infrastructure technology and business process. From a functional perspective, IDM infrastructure must address the need to manage identity over its entire life cycle, consistent with business objectives, policy, and relevant regulations.

The IDM market is approaching a crossroads: the complexity of managing users across organizations is increasing; end-user resistance to being held responsible for managing credentials is increasing; security requirements to preserve privacy and prevent identity theft are increasing; and, IT budgets for the technology are decreasing. Most IDM tools enforce corporate security policy by offering secure badging, authentication, provisioning, and access control. Advanced features can build bridges between systems. For example, password management bridges authentication and provisioning systems to simplify end-user management of multiple application accounts.

Today, most companies manage identity on a per-application basis. But identity must become more persistent through the continuum of any given business process, spanning not only multiple applications, but also multiple organizations. Historically, enterprises have made attempts to treat the symptoms of the IDM problem with localized solutions. IDM tasks are typically under the purview of several departments in an enterprise. Access management tasks are also typically handled manually and can take staff over several departments and many man-hours to manage.

1. HIGH-LEVEL DEFINITION

Within an enterprise, the components of IDM can function independently, or can be loosely or fully integrated depending on the system’s design and architecture. Each component is described below

Identification. The identification function can be broken down into two processes:

ID Verification. ID Verification refers to establishing identity by verifying that an individual in question matches the claimed identity through processes such as ID and biometric data capture, ID document authentication, ID searches and matching, background checking, and ID validation.

Credential Management. Credential management refers to the issuance and management of a credential that binds the person to the identity for the purposes of authentication when challenged for access control through processes such as badging, smart card issuance, physical and logical credential issuance, and card management.

Access Management. Access management refers to the user life cycle management associated with the creation, updating and deletion of user identities and to the distribution of related equipment needed to support those identities. It consists of processes such as privilege and access granting and privilege lifecycle management and roles based provisioning.

Access Control. Access control refers to the use of authenticated identities to gain access to security sensitive systems and physical areas to include the operation and management of logical Access, physical access and federated access through secure authentication.

2. TAXONOMY OF IDM

Because the IDM marketplace includes such a variety of often overlapping products, the following taxonomy is presented as a framework for the marketing analysis. Exhibit 1 shows an Identity Management Taxonomy comprised of three major functions, which, in turn, are explained by business processes. Various component combinations of technology systems and software can be integrated as service offerings to support the business processes and are shown at the bottom of the Exhibit.

Identification and Authentication: Identification and authentication refers to the processes involved in establishing identity, verifying that an individual in question matches the claimed identity and, in turn, providing a credential that binds the person to the identity for the purposes of authentication when challenged for access control. Identification and authentication consists of the following four processes.

- *ID Capture/Enrollment.* Consists of capturing the data and physical attributes that define identity such as taking a photograph, creating an electronic record of fingerprints, recording profile data such as social security, license and passport numbers and starting the user's enrollment data file. Equipment and systems needed to execute the processes can include ten-print finger and hand scanners, and digital cameras and signature pads tied to credential (e.g. smart card) enrollment systems.
- *Identity Verification and Validation.* Consists of verifying a person's identity by submitting fingerprints to state police and/or the FBI for checking against criminal records databases and running demographic data and/or social security numbers against economic records history databases. Equipment and systems required to execute these processes include the automated interfaces to the FBI, State Police and, soon, the Department of Homeland Security. In addition there are equipment (such as document authenticators) and services that authenticate license, passport, immigration documents, and other breeder documents.
- *Identity Profiling.* Consists of searching and querying systems and databases to pull or create records and/or histories for more extensive identity and background checks and for investigative purposes.
- *Credential Issuance.* May involve, first, binding the user's identity to the credential by checking the user's biometric against the one on file from the ID Capture/Enrollment process. The user data file is then completed and the card (or other token) is initialized and loaded with applications and credentials tailored to user requirements. Printing the photo and applying additional counterfeit foils to the card completes this process. Required equipment can include card issuance and personalization systems, smart cards, card and biometric encoders and readers.
- *Credential Management.* Involves tracking the lifecycle of the card and includes re-issuing lost, stolen and malfunctioning cards, updating credentials and applications, and revoking cards upon employment termination. In the case of updated credentials, this process is informed by the Privilege Access and Granting process (following section) and provides data to the Credential Issuance process. A card management system is needed to support this process in large enterprises.

Access Management: Access management refers to the user life cycle management associated with the creation, updating and deletion of user identities and to the distribution of related equipment needed to support those identities. Access management consists of the following processes:

- *Privilege and Access Granting.* Consists of the assignment of roles and privileges and registering them in access authorization applications. Software system applications needed to support privilege granting as well as user lifecycle management (see below) can include provisioning applications, password management applications, directory products and web services platform applications. Provisioning software can provide for the propagation of user identities and roles throughout the authorization and control components of the Identity Management System.
- *Privilege Lifecycle Management.* Involves updating user profiles, updating, revoking and suspending privileges and updating user directories.

Access Control: Access control refers to the use of authenticated identities to gain access to security sensitive systems and physical areas. It consists of the following three processes:

- *Logical Access.* Consists of access to enterprise IT systems and applications, including networks, portals, intranets, extranets, the Internet as well as remote access to the enterprise domain. Required equipment and systems can include smart card middleware, password management applications, single-sign-on (SSO) software, web services software, smart card logical readers and PKI applications.
- *Physical Access.* Includes exterior and interior access to enterprise buildings and facilities, secure areas, and property parking facilities. Required equipment and systems can include RFID card readers, controllers/panels, servers, transaction authorization applications and electronic door locks.
- *Federated Access.* Involves the extension of access privileges across external logical domains and external facilities. The term federation is used to describe the manner in which users groups agree to cross-domain interoperability through shared standards and processes for authentication and access control. Equipment and systems needed to implement a federated identity system can include federated domain servers, local enterprise interfaces to the federated system and credentials standardized to federated operating rules.

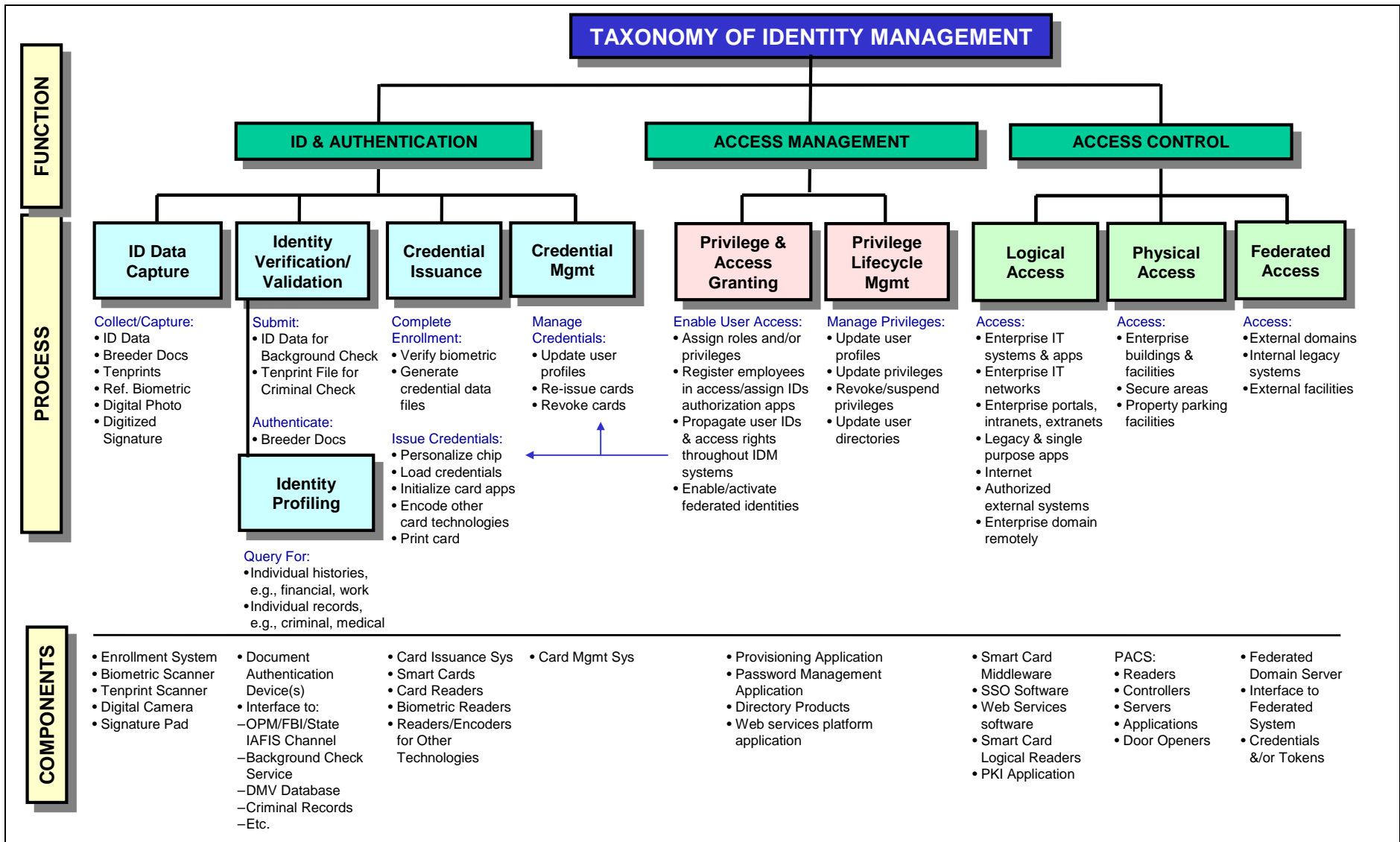


Exhibit 1: Taxonomy of Identity Management