The Challenge of Identity Services

Version: 1.0, Sep 12, 2008

AUTHOR(S):

Kevin Kampman
(kkampman@burtongroup.com)

TECHNOLOGY THREAD:

Identity Management

Conclusion

The opportunity to establish consistent and interoperable identity management (IdM) capabilities within and between organizations is compelling, particularly given the challenges and difficulties that organizations have experienced to date. While the vendor community has made progress toward internally consistent solutions, these are not keeping pace with the changing needs of businesses, customers, and society.The IdM industry has an opportunity to reduce integration challenges and demonstrate value to customers by removing barriers to adoption and interoperability. Working with the Identity Services Work Group (ISWG) to promote consistent characteristics and interfaces can lead to broader understanding and cooperation and, ultimately, to more effective solutions.

BURTON GROUP 7090 Union Park Center · Suite 200 · Midvale, Utah 84047
P 801.566.2880
F 801.566.3611
www.burtongroup.com

Table Of Contents

Synopsis

Burton Group is facilitating discussions with organizations working on enterprise identity management (IdM) initiatives. These initiatives involve the major IdM vendors and represent significant investments on the part of the organizations. The key issue emerging from these efforts is that achieving interoperability between solutions is challenging and expensive. This is due to the lack of common interfaces and capabilities. The organizations recognize that the current situation is untenable for them and that change is necessary. Their perspective is that an identity services model is a viable alternative.

A service oriented architecture (SOA) approach to identity is compelling. It can provide commonality, portability, explicit interfaces, reduced integration costs, and improved interoperability between products. It can also make the implementation of IdM solutions more straightforward and effective. Although a number of standards contribute to IdM objectives, they are inadequate to address the breadth of capabilities required for a comprehensive IdM deployment.

The Identity Services Work Group (ISWG), an informal group of companies formed to discuss IdM challenges, recognizes that it needs to work with business, the IdM industry, and the standards community to further its goals. It has opened the effort to participation by selected vendors and is working to advance its efforts to a broader community of interest.

Analysis

Burton Group has been facilitating discussions with a number of organizations that are executing identity management (IdM) initiatives. This group of global enterprises, including financial services, manufacturing, telecommunications, and government agencies, faces a wide range of challenges. These enterprises work with most of the IdM vendors and have acquired sufficient background to develop a picture of the IdM terrain and the road toward a solution. The participants in the Identity Services Work Group (ISWG) are committed to defining capabilities that move them beyond their current integration challenges and enable them to keep pace with their changing business environment.

What's the Problem with IdM?

IdM has made significant strides toward a consistent view of identity information within enterprises. The more we accomplish, however, the more we see that needs to be done. Federation, for example, represents a bellwether for what companies can accomplish, but also for what needs to change. The exchange of identity information within and between businesses can be problematic; application interoperability is a huge challenge. Establishing trust and minimizing risk remain fundamental concerns. Finally, interoperability is a fairly recent expectation for information and for applications, so it is no wonder that the IdM industry isn't there yet.

In the midst of this situation, businesses need to move forward. Mantras like flexibility, agility, and adaptability compete with expectations like consistency, accountability, compliance, and the capability to be audited. Good enough isn't, anymore.

The vendor community is also challenged to keep pace with change. Most of the commercial IdM solutions on the market today offer a suite of capabilities, but seamless internal interoperability is rare, and vendor-to-vendor interoperability is a significant integration exercise. Pair this situation with an organization's diverse requirements, legacy environments, and varying priorities and the situation for information technologists is daunting, at best.

Enter service oriented architecture (SOA). This approach offers a mature perspective that orients products and applications with a framework of loosely coupled, interoperable capabilities. However, we have to do some growing up to get there. We can't easily divorce ourselves from where we already are for the promise of something better—at least, not completely. Furthermore, putting everything on the web is not sufficient. Web services are just part of the equation; much of the practical integration must take place in the bowels of the existing platform, application, and information environment. The bottom line is that SOA or any other approach comes at a cost, and we'll still need to deal with the status quo.

The promise of identity services is to simplify the integration of IdM features and capabilities. It is not as though we can't make today's products work. The question is: At what cost (money, time, and effort)? SOA provides guidance toward the use of identity services, particularly in terms of addressing the capabilities of what we already have. Among the many standards and protocols to choose from, none make up the service. The Lightweight Directory Access Protocol (LDAP), for example, provides some rudimentary capabilities that support simple authentication, but these fall short of a fully capable authentication service, particularly when the bar is raised for business-to-business or higher-risk interactions.

Can We Solve This?

One of the ISWG participants characterized its IdM integration and interoperability challenge as “accelerating the car with one foot on the brake.”

Although the company knows where it would like to go, its progress is fairly constrained by its current situation. It became clear in Burton Group's conversations with the participants that a new point of view is needed. The idea of identity services is attractive, but the ISWG membership is concerned that most of the discussion is coming from particular vendors rather than the industry at large. A proprietary model is not sufficient or desirable. The approach needs to represent a point of convergence for all vendor solutions rather than a scattered collection of dissimilar offerings.

There is really nothing new about this perspective. At the same time, vendors are being challenged to address specific customer expectations and project challenges that run counter to a high-level, interoperable approach. Businesses need to approach this challenge with high-level interoperability in mind and be willing to make short-term compromises to achieve longer-term goals. Before any discussion of technology takes place, mutual commitment to shared outcomes is required.

A SOA approach is compelling for identity services. It addresses many of the high-level requirements that the ISWG participants have expressed, including:

- Reusable, portable, and interoperable solutions
- Vendor independence
- Reduced need and level of effort for integration
- "Invest and install once, interoperate everywhere"

Information technology (IT) recognizes that it needs to change direction. For example, if a business requires the means to deliver more-targeted capabilities to its customers, then IT—rather than developing new database solutions—needs to enable the business to analyze customer characteristics to achieve that focused approach. If an existing solution is insufficient, IT should strive to find a solution (by acquisition or sourcing) that can meet the required level of performance and capability, and not try to retrofit the existing solution to meet more-demanding requirements.

Ultimately, identity services should facilitate the exchange of an identity principal and policy information to address multiple business scenarios. In the absence of a common approach, tying together disparate environments places the onus of development and integration efforts and costs on customers. Continuing down this path is an untenable situation for the ISWG participants. They have expressed the need to partner with the vendors and standards community to embrace change. Business must also embrace this approach and require conformance of the organization to the same framework.

While moving toward a common framework, organizations can meet business needs using short-term alternatives. Outsourced integration and virtual directory technologies have been identified as methods to simplify integration, and their benefits are viable. Whether they are compelling as long-term solutions remains to be seen, but they represent alternatives that can support a business's objectives as it moves toward a longer-term objective.

The "Identity Services Framework" section of this overview describes, at a high level, the major identity services capabilities recognized by the ISWG:

- Endpoint administration
- Step-up authentication
- Authorization
- Attributes
- Tokens
- Federation
- Context and policy
- Session
- Logging and audit

In many cases, these correspond to existing IdM features. Others, such as context and policy, are not articulated as well. Another consideration, the characteristics of relationships, broadens the set of capabilities for communities of interest and the business-to-consumer space.

As the participants described the functions, boundaries, and characteristics of these services, their interdependencies became obvious. Identity services need to be considered holistically—even if the component services come from multiple sources—and their interactions must be well understood. The group decided that it would be necessary to gather the perspectives of a wider community that includes vendors and standards bodies, in order to leverage previous work and to gain consensus on service capabilities.

Recommendations

In June 2008, at Burton Group Catalyst Conference North America in San Diego, the findings of the ISWG discussions between February and June 2008 were presented. The group issued an invitation for broader participation; in particular, to selected vendors and standards body representatives. This effort is ongoing, with the objective to promote an enrollment and authentication architecture at Burton Group Catalyst Europe in October 2008.

The ISWG feels that a transparent effort will benefit the entire IdM industry and recognizes that the challenges to be addressed are offset by the perceived benefits. A previous example of industry collaboration yielding similar benefits is the network infrastructure model in which adoption of a common protocol and services (Transmission Control Protocol/Internet Protocol, or TCP/IP) provided the foundation for network interoperability. By aligning the requirements and interests of multiple parties (customers, vendors, and standards bodies), the ISWG anticipates that its coordinated effort will harmonize service dependencies, inputs, and outputs, with the potential to impact IdM in a fashion similar to TCP/IP.

A coordinated effort will help to mitigate the concerns of the ISWG membership by providing consistency and lessening the business risk associated with identity. Conformance helps the vendor community by simplifying development requirements and adds value for customers by limiting their investment risk and integration requirements. Vendors can differentiate themselves by streamlining integration capabilities, offering better performance, and strengthening their overall IdM offerings. These benefits are extant even when services are provided by third parties.

In Figure 1, the major identity services capabilities are rated according to their maturity. They are described in more detail in the "Identity Services Framework" section of this overview. Authentication, authorization, attributes, tokens, and federation represent the areas where dependencies, recognized challenges, and industry experience are sufficient to begin the initial effort. Longer term, session, context, and policy services are candidates for examination. This approach can provide tangible benefits and guidance based on capabilities that are already in place.

Initially, the ISWG, in conjunction with select industry participants, will focus on clarifying common identity-related attributes and develop requirements statements and use cases for enrollment and authentication. Additional opportunities exist to identify barriers, gaps, and alternative approaches, institute development, and conduct interoperability demonstrations.

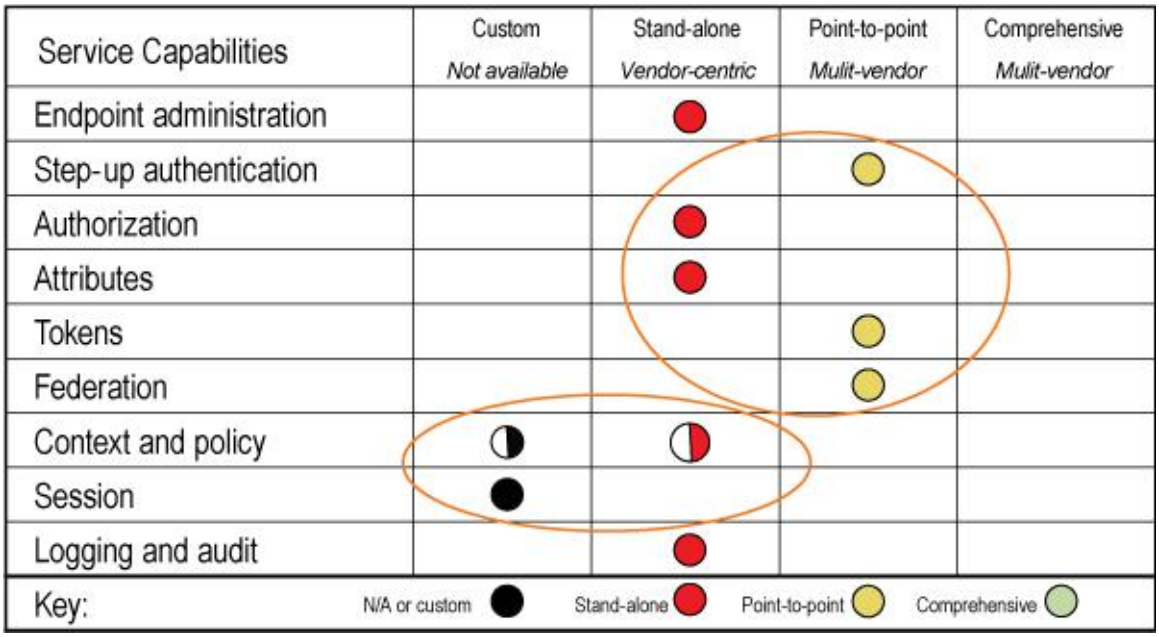

Figure 1: *Service Capabilities and Opportunities*

The Details

In 2007, Burton Group began investigating customer experiences with identity management (IdM) and service oriented architecture (SOA). Several companies agreed to work together in a private effort to develop services expectations, and the results of that initial survey were presented at the Burton Group Catalyst Conference North America in San Francisco that year. Further activities were limited until late in 2007, when a number of organizations expressed their interest in continuing the effort.

In February 2008, Burton Group and these organizations—a number of new members and several of the original contributors—established the Identity Services Work Group (ISWG). The group agreed to follow the original pattern of activity: to participate and share information and experiences under the Chatham House Rule. This rule states that "When a meeting, or part thereof, is held . . . participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." Using this principle and operating under mutual nondisclosure agreements, the group has also established a private exchange point for member information at https://identityservices.wikispaces.com/.

The Community

In July 2008, the ISWG membership included more than 15 organizations. These represent global financial services, telecommunications, and manufacturing companies. Professional services, governmental agencies, and health services firms are also participants. We anticipate additional participants from the vendor community as the effort progresses.

For the most part, the customer organizations have targeted one or several capabilities for Identity Services such as authentication, authorization, or federation. They have invested in internally developed or third-party vendor solutions and have working relationships with (and products from) the major IdM vendors. Their experiences have been challenging: They recognize that their investments in identity services will not result in a multivendor, general-purpose solution.

Charter and Objectives

The ISWG set forth the following charter for its activities:

> Organizations recognize the need for the unambiguous expression of identity. Identity can represent a physical individual, a collection of individuals, a logical entity, a resource, or a capability. Identity is a fundamental element for establishing and maintaining business relationships and for describing the credentials, capabilities, and responsibilities of parties to a relationship.
> There are a number of identity capabilities available, including directory and security services. None of these are sufficiently authoritative to satisfy the need for an unambiguous expression of identity in multiple contexts. They are limited by their perspectives as well as their ties to particular technologies. These limitations indicate the need for a broader and more abstract set of capabilities. The identity-related vendor community has indicated the need for direction for development in this area.
> The purpose of the ISWG is to establish requirements for the articulation of identity in web services and other environments. These requirements should correspond to business functions, activities, and expectations and demonstrate how these will be accomplished in the web services context. The ISWG will identify what identity-related capabilities are required. How these capabilities are accomplished technically is specifically out of scope for this effort.
> The ISWG will develop a set of business-driven scenarios which describe what identity information is needed and how it is used. These scenarios should correspond to the lifecycle of a relationship, including creation, functionality, maintenance, and termination. The scenarios should be sufficient to describe a broad set of situations as are practical for the composition of ISWG membership. The scenarios should provide sufficient examples of what information is needed within a well-managed IdM environment and how it is used in order

to provide requirements for the technical and vendor community to develop satisfactory and workable solutions.

The ISWG will promote their requirements to a broader community of interest to solicit feedback and additional contributions and will maintain the information throughout the course of development, publication, and promotion. The ISWG will also provide support to the business and vendor community throughout the development of solutions, as well as to standards bodies seeking to standardize their efforts.

Some Definitions

Burton Group recognizes that identity-related terminology in the SOA space has created significant industry confusion. In addition, certain vendors have recently trademarked certain terminology, making it even more difficult to clearly express services capabilities. At its Catalyst Conference North America in July 2008, Burton Group set forth the following definitions to clarify these capabilities:

- **Service-Oriented Identity ():** A service-oriented approach to IdM. A software design discipline in which application and infrastructure functionality are implemented as shared, reusable services. Each service implements a discrete task, and any application that needs to accomplish that task uses the shared service to do so.
- **Identity Services:** Technologies and infrastructure that enable SOI, including shared services, open standards, web services, and so forth.
- **Identity on Demand:** An outsourced, hosted, Software as a Service (SaaS) model. The software is often delivered over the Internet and is "leased" from the service provider (SP). The SP maintains the software, which is delivered to multiple lessees.
- **Identity Provider:** Third-party provider of identity data (e.g., OpenID; A number of providers are identified at the OpenID website; you can also build your own OpenID identity provider capability.)
- **Identity Service Provider (IdSP):** Similar to a managed service provider (MSP). The IdSP hosts the software (either on or off site). The IdSP manages all or most aspects of the project and implementation for the customer, but the customer maintains ownership of the software license and any associated information. Software customizations are allowed.

These definitions provide guidance to the industry and to customers establishing a framework for identity-related services.

The workgroup participants conducted an initial discussion of their own identity services needs in order to establish areas of interest. These areas include:

- **Principals:** The registration and management of information about identities internal and external to an organization
- **Profiles:** Characteristics of principals, expressed as attributes or the results of conditionals, that describe their relationship in a particular context
- **Common Identifiers:** The establishment of attributes that uniquely identify a principal, often described as a globally unique identifier, or GUID
- **Directory Services:** The range of services (including network operating system, enterprise, meta- and virtual directories) used to consolidate and publish identity information
- **Federation:** Authentication and authorization across disparate applications and security domains; also between organizations
- **Provisioning:** The establishment, maintenance, and termination of user privileges to platforms and applications
- **Step-up or graded authentication:** Determination of an identity using a variety of mechanisms ranging from simple (e.g., user ID and password) to strong (e.g., multifactor) authentication based on the circumstances of the access desired, which may involve requiring additional verification as the risk profile increases
- **Token services:** Physical and logical artifacts representing a relationship with a principal
- **Authorization:** The expression of what an authenticated principal is allowed to do within a particular context

- **Role management:** An expression of responsibilities or capabilities that enables more effective administration and enforcement of policies
- **Event management:** Assessment of activities against a risk profile to determine appropriate responses
- **Auditing:** Maintaining and analyzing logs and transaction information to identify who conducted specific activities at a specific point in time
- **Trust:** The ability to describe a relationship between principals and businesses with other principals and other businesses and clearly articulate the responsibilities and constraints of the relationship in a manner that is mutually beneficial and agreeable

  Trust is an enduring problem; the farther endpoints are from each other, or if a relationship is not well defined, the more difficult it is to establish trust. To address these challenges, intermediate relationships may be used to establish trust, but this approach can be problematic. In mathematical terms, trust is not transitive. If A trusts B, and B trusts C, this does not imply that A trusts C. (For example, if Mary trusts Provider, and Provider trusts Peter, Mary does not necessarily trust Peter, unless this is explicitly understood as an objective, or to use a contemporary analogy: The enemy of my enemy may *not* be my friend.)

The ISWG participants indicate that significant internal and vendor attention is paid to identity services. However, the participants have raised concerns about common challenges they face. One is a lack of consistency between vendor approaches and solutions that has resulted in a lack of interoperability—a vendor's solution doesn't necessarily work with, or in the same manner, as another's. Because they usually have multiple-vendor solutions, this means that these participant organizations experience difficulty integrating solutions between vendors. This situation also results in the need for the development of customized, rather than consistent, service interfaces. Most of the integration challenges and associated costs are borne by the customers. These costs are significant and put the customers in an untenable situation.

Another challenge relates to the intersection points of applications and repositories. Since these delineations are not clearly articulated, different vendor solutions impose varying assumptions and dependencies on underlying technologies. This lack of alignment demonstrates another challenge for integration and support of multivendor environments.

A major issue for organizations involved is the disparate nature of their existing IdM environments. Most of the participants are still trying to bring order and clarity to their identity situations, each of which has its own problems to solve and priorities to address. For example, a logical coordination point for identity information is a key milestone in an IdM infrastructure. Many companies are still trying to address this and have indicated that they are still some distance from a mature and consistent view of identity information.

The lack of consistency and clearly articulated boundaries results in environments that are challenging to implement and expensive to manage. The lack of clarity also results in “lots of pain” for the organizations making investments today. This is clearly a situation that needs to change in order to move past the current challenges of IdM and to arrive at a common framework that is viewed as an advantage rather than an impediment to business objectives.

Identity Services Framework

As the ISWG formed and shared its experiences, it became apparent that each organization was addressing challenges specific to its particular business needs. The maturity of the participants varies widely; some organizations are just getting started, others are much further along in adopting solutions. Among those that have experience, one organization's focus may be widely different than that of another.

In order to gather information and establish objectives, several face-to-face meetings were held on one participant's premises in Toronto, along with concurrent or stand-alone teleconferences. The initial goal was to develop use cases for identity services based on existing participant project information. However, we determined that this was premature given the wide range of expectations and levels of experience. Although the goal of the group was to collect and share experiences, the differing levels of maturity, available documentation, and business limitations restricted the group's ability to produce a comprehensive overview between the inception of the effort and the Catalyst Conference North America. An additional challenge we faced was the abstraction of services capabilities. It became apparent early in the definition process that because of service interdependencies, a breadth-first examination of their capabilities was necessary prior to a deeper evaluation of individual services.

After assessing the overall situation, our most productive activity was to inventory where each organization stood regarding its identity services needs and priorities. From this discussion, a pattern or framework of identity services emerged. This framework includes the following capabilities:

- **Endpoint Administration:** This involves managing the lifecycle of a relationship with a principal. An endpoint could be a provider or an organization with which the principal has a relationship. Entailing the manual and automated identification, vetting, and instantiation of a principal in an IdM system, this capability may also include the evaluation and verification of a principal's identity.
- **Step-up or Multifactor Authentication:** Authentication is the process of identifying a principal to a particular level of certainty. Levels of authentication are based on risk profiles. Simple authentication relies on a user name and password combination and has a low risk threshold; stronger authentication requires a combination of something you have and something you know. An example of the latter would be a bank card and personal identification number (). Based on the activity being performed or the access desired, a principal may be asked to produce a simple or strong form of authentication or to move from a simple to a stronger form of authentication (step-up or escalation). An authentication service identifies a principal—with an accompanying degree of certainty.
- **Authorization:** Authorization demonstrates what a principal is allowed to do. If an authorization is sufficient, the principal is granted access to the desired application and information resources. Authorization can be coupled to the degree of authentication. For example, an authenticated principal who wishes to do something that has a higher authorization may be dynamically required to produce an accompanying stronger form of authentication. An authorization service indicates the resources that a principal can access based on a level of authentication.
- **Attributes:** Attributes represent the logical characteristics of a principal. An attribute service provides authoritative information about a principal when it is needed for a particular purpose, in accordance with policies that govern acceptable use of that information. An attribute service may mask or protect the authoritative information by asserting that it meets certain criteria (e.g., an age limit or membership in a group).
- **Tokens:** A token is a physical or logical representation of a principal that provides a level of assurance of the authenticity of the user. A token can be logical, such as a public key infrastructure (PKI) certificate, Kerberos ticket, or browser artifact. A token can also be physical, such as a smart card. A token service is responsible for the management, security, and verification tasks for tokens.
- **Federation:** A collection of capabilities, federation results in cross-domain authentication and authorization. Although often thought of as a single sign-on mechanism, its capabilities are more extensive, particularly in terms of supplying authorization information. Federation services accommodate the bidirectional request and response activities necessary to enable access within and between enterprises.
- **Context and Policy:** Each of these service activities takes place within a set of boundaries and conditions that, in traditional situations, are frequently implicit or assumed. For example, access to a host application might only be accomplished from a connected terminal, so an assumption could be that the user is inside the physical constraints of a controlled facility. As we approach situations from a general-purpose perspective, it becomes necessary to make these conditions and characteristics more explicit. Context helps to define a relationship—for example, temporal or business characteristics. Policy imposes constraints; for example, conditions that must be satisfied for a particular capability to be provided. In summary, context and policy services articulate the relationships and conditions that govern service functions.
- **Session:** A session represents a particular interaction between a principal and an application or a capability. A session service is responsible for the establishment and termination of an interaction and the coordination of all the pertinent capabilities required to satisfy the conditions required for that interaction.

- **Logging and Audit:** In order to ensure that an interaction is accomplished properly—and to certify the relevant characteristics of that interaction—it is necessary to capture its state and conditions. This capture is performed by a logging service. The subsequent examination of this information is accomplished by an audit capability or service. An audit service satisfies standard and ad hoc reporting requirements on interactions, including exceptions and violations. The associated information is archived and protected from alteration or deletion according to business requirements.

What About Standards?

A typical question that came up during our discussions was "Doesn't *this* standard solve *that* problem?" A consistent perspective that came out of the initial and ongoing effort on identity services is that "the standard (or protocol) is not the service." For example, while the Lightweight Directory Access Protocol (LDAP) addresses how to access information stored in a directory, and the Security Assertions Markup Language (SAML) enables authentication, neither represents all of the capabilities required of a service. Understanding what information is in a directory and how it is meant to be used or what information is needed to satisfy a login request goes beyond the capabilities of a protocol.

Services leverage protocols. One of the challenges in this effort is to determine whether or not the needs of a particular service are satisfied by one or several protocols, or if additional or refined capabilities are required. For example, is an Extensible Access Control Markup Language (XACML) assertion sufficient to establish authorization to a partner's application, or is additional information provided by an LDAP query or token validation required?

Another challenge is the selective adoption of protocol capabilities. Vendors may adopt certain features of a protocol, but not embrace it completely. One of the participants cited the adoption of SAML assertions, but not SAML profiles, as an example. The question this raises is whether this approach is expedient, represents the best or most useful characteristics of a standard, or results in the ultimate incompatibility of a solution. The identification of mandatory and optional capabilities for standards adoption would address this concern.

Obviously, more questions have been asked than have been answered. Many situation-specific nuances can only be exposed by establishing use cases that describe the objectives, processes, and exceptions that may arise. Disclosure and examination of these is a necessity for a meaningful definition of service capabilities and the ability of existing standards to meet these needs.

In order to assess the challenge facing the industry, Burton Group used the identity services capabilities described in the "Identity Services Framework" section of this overview as a guideline to establish a preliminary assessment of the current marketplace. In Figure 2, we developed a functional maturity matrix for these capabilities, which provides a qualitative perspective that describes vendor and organizational capabilities, as well as their adoption.

Service Capabilities	Custom *Not available*	Stand-alone *Vendor-centric*	Point-to-point *Mulit-vendor*	Comprehensive *Mulit-vendor*
Endpoint administration		●		
Step-up authentication			●	
Authorization		●		
Attributes		●		
Tokens			●	
Federation			●	
Context and policy	◑	◑		
Session	●			
Logging and audit		●		
Key:	N/A or custom ●	Stand-alone ●	Point-to-point ●	Comprehensive ●

Figure 2: *Identity Services Functional Maturity Matrix*

The matrix describes each capability, in a range from the least to the most mature:

- **Custom:** If it is available, a custom solution is one that is developed for a particular customer situation. It may have been provided by the customer, a third-party integrator, or by the vendor. These solutions are often characterized as "one-offs" and are particularly expensive to implement and support.
- **Stand-alone:** A stand-alone solution is one that exclusively supports a particular vendor's platform and applications.
- **Point to point:** A point-to-point solution provides support for more than one vendor, but does not provide universal coverage across all environments.
- **Comprehensive:** A comprehensive solution provides generalized support for a wide range of vendor solutions. While none of these service capabilities has reached this stage of maturity, this represents the goal state.

As Figure 2 demonstrates, the areas of authentication, tokens, and federation services are fairly mature. Administration, authorization, attributes, and audit capabilities tend to be vendor specific. Context and policy capabilities are moving from a custom to the vendor-specific category, while session services are highly specific.

An additional delineation or perspective in the services area today is that both Sun's Java and Microsoft's .NET are intended to provide a high degree of abstraction and portability. Although .NET is specific to the Microsoft Windows platform, Java is more general-purpose. However, they represent two distinct and competing camps; both represent sizeable constituencies, frequently within the same organizations, and each must be acknowledged separately since they are not interoperable.

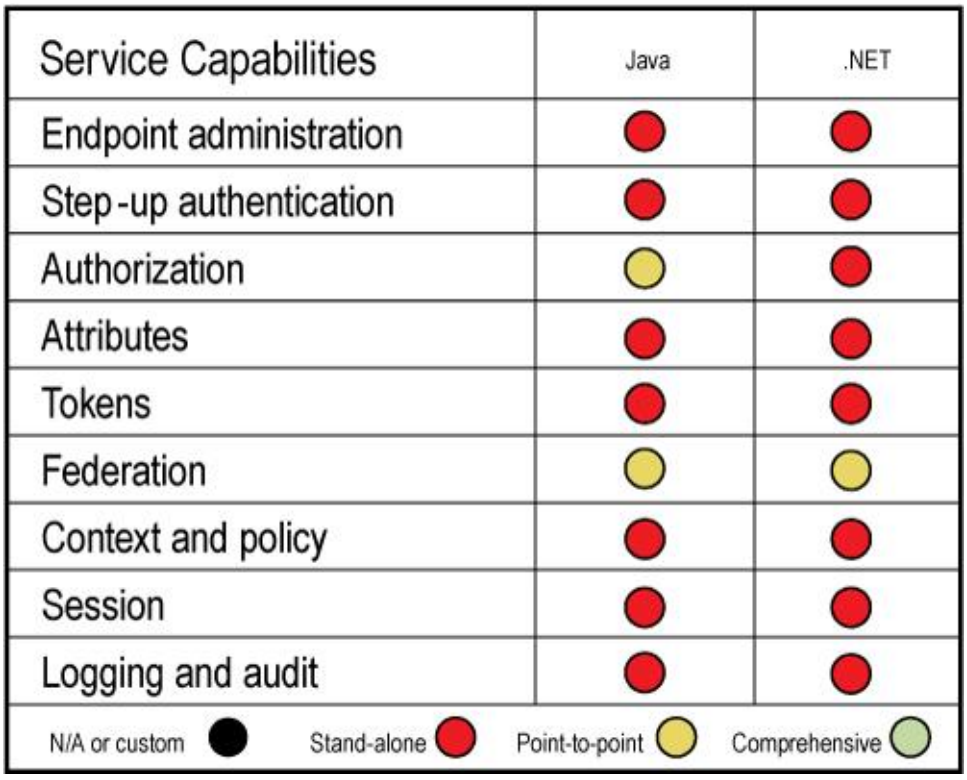

Figure 3: *Identity Services Environment Maturity*

Federation services are reaching maturity and adoption in both environments (as demonstrated in Figure 3), thus providing this capability in multiple-vendor situations and between Java and Microsoft platforms. Authorization is also fairly mature in the Java space. Capabilities in other areas are more stand-alone today, representing a less-mature situation that corresponds to Figure 2. Taken together, Figures 1 and 2 illustrate that the opportunity for progress in identity services is significant and that a wide gap exists between the current and desired future state. To accomplish a modicum of product interoperability will require coordinated initiatives and vendor-customer cooperation to articulate the required expectations and functionality.

The Objectives

Any journey involves knowing one's destination. The business perspective of identity information is a coordinated lifecycle (see Figure 4), beginning with the enrollment of an identity, the exchange of identity information, and its maintenance. This all takes place under the auspices of a business relationship, managed and conducted according to the policies and the context that characterize that relationship.

For the ISWG participants, their objectives are aligned with most enterprise IdM initiatives. The first objective is to get one's identity house in order, that is, to organize the information and the processes associated with its enrollment, maintenance, and exchange. To accomplish this requires a logical view of useful, authoritative identity information. This information should be persistent and unambiguous and should uniquely identify and describe a principal or resource. Attributes should be authoritative, or link to the authoritative source.

Characterizing Identity

A principal and its relationships are described by meaningful characteristics. What these are and how they are collected and maintained over time is determined by the context of the relationship, and the policies that govern the relationship.

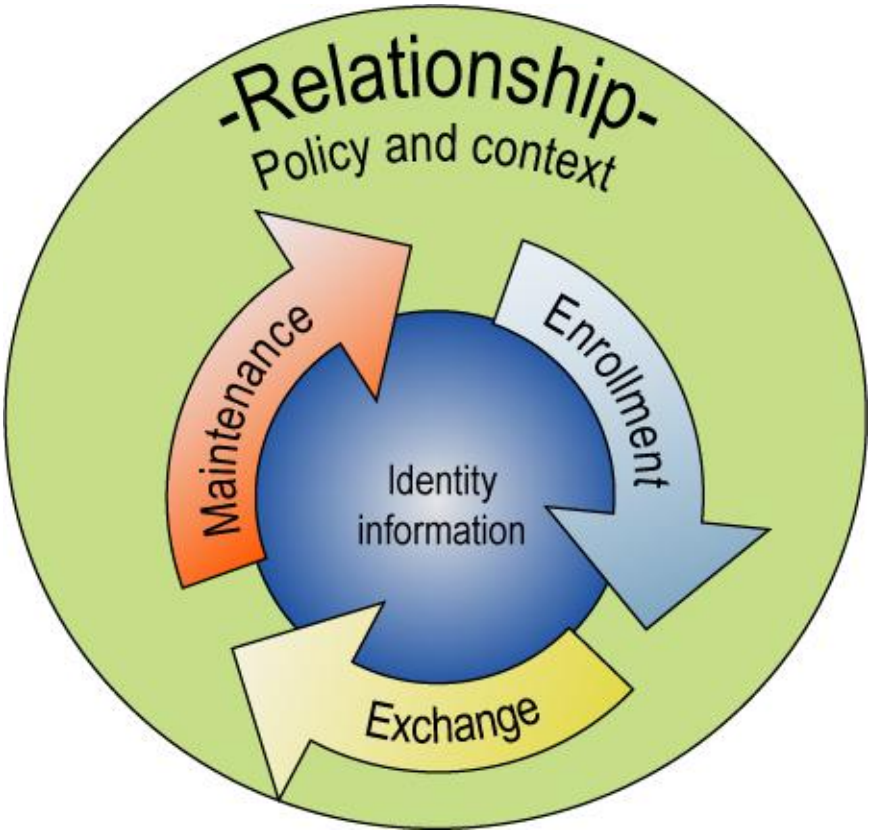

Figure 4: *The Business View of the Identity Lifecycle*

Identity characteristics should be general-purpose in nature, avoiding transactional, application-specific, or private information. For example, the extrapolation of access privileges or volatile characteristics from an application or repository should be avoided. These specific characteristics are better maintained in their own environment, although they can be incorporated by reference in an identity repository if necessary.

The relationship of the identity to the organization should be reflected in the characteristics, including lifecycle features (such as active or inactive, type of relationship, and sponsor or owner). Attributes that facilitate identity abstraction and support policy evaluation should be used to enable portability. For example, roles, geography, and similar characteristics are useful and beneficial if their purpose is well understood and maintained. Whenever attributes, policies, and rules are employed, they should be used consistently and satisfy the needs of all stakeholders, including information security, audit, and compliance.

Employment of recognized objects and attributes simplifies the exchange and interpretation of information. Identity information should represent something meaningful between and throughout enterprises and communities. Attributes should be explicit and well understood. Overloading, alternation, or misuse of attributes should be avoided, as well as the use of attribute values with embedded meanings (e.g., "the first four characters are the department code, the next three are the building, and the last four are the floor and post number"). In a real situation, a company used an attribute defined in this way with wide-ranging usage dependencies and encountered system and application failures when the owner of the attribute decided to redefine the elements. For widely leveraged or critical attributes, it is helpful to understand and manage dependencies by developing a create-read-update-delete (CRUD) matrix to identify who controls and who depends on attribute information.

Evaluating a policy at the time a decision is made is more effective than maintaining an attribute that represents an outcome in the identity repository, especially if the supported policy changes or becomes obsolete. A specific policy may state that a prearranged vendor is used by employees at a particular management level in a certain region when renting transportation. In this example, providing the level and geography information for evaluation is more appropriate than explicitly storing a vendor attribute. The latter requires more administration while only satisfying a narrow purpose.

Start at the Very Beginning . . .

Although different organizations have different expectations and focal points, the collective view of the ISWG participants is that identity services should span the entirety of relationships. Individual organizations make assumptions about identity, such as assuming that an identity is already registered or provisioned. The broader perspective is that all of the following conditions are satisfied at one point or another.

First and foremost, identity services should facilitate identity enrollment. Enrollment begins with verification of a principal's identity assertion. In other words, "This is who I am, and this is how I prove it."

In many situations, identity verification is a manual process, involving the evaluation of government-issued or other forms of identification. In other situations, verification relies on the presence, quality, and history of relationship artifacts, such as a bank or utility account or a credit history. The nature and quality of verification depends on the level of risk (or degree of trust) that is acceptable for a particular relationship. Verification is fundamental to all subsequent activities associated with the identity; understanding an organization's requirements and procedures for verification will identify areas of certainty as well as dependencies on these processes and information. It will also help to ascertain if the process and information is sufficient to be leveraged for broader purposes, such as business-to-business exchanges.

Processes that depend on verification include registration, authentication, authorization, provisioning, and audit. Each of these processes should be conceived of as a service in the sense that it is sufficiently abstract, has a consistent and corresponding interface, and supports the collective process and technical requirements of its subscribers.

Registration is the point at which an identity and relationship are established. Verification and registration may be accomplished in parallel, such as when a user provides information to sign up for a web account or service, and the furnished information (e.g., address and financial information) is validated. The goal of registration is to capture sufficient information to characterize an identity within a bounded relationship. Registration can be accomplished in a self-service or assisted manner.

Once an identity is validated and registered, the characteristics associated with the relationship become available for appropriate purposes. Sufficient characteristics of the identity and the associated relationship should be exchanged to satisfy the needs for authentication and authorization; in some cases, this will be done manually or out of band (e.g., issuing a physical token). In most situations, authentication and authorization also require provisioning an account to an application or resource.

Authentication determines that principals are who they say they are, based on a preestablished set of authenticators, such as an ID/password pair. When stronger authentication is required, more stringent mechanisms are employed. In any case, the degree of authentication should be balanced to the risk involved. If, in the course of a session, the current means of authentication is insufficient, step-up authentication enables an additional means of authentication to be instantiated.

Authorization is closely coupled with authentication. For static authorizations, if we know who someone is, we can then determine what they are allowed to do. Authorization assesses that the right conditions are extant using characteristics of the principal, the relationship, policy, and context. For dynamic requests, authorization processes can determine if additional authentication or other criteria are required and direct the appropriate services to either present what is needed or deny access.

Provisioning is used to establish and manage access to resources and to solicit advance approvals. Provisioning represents coarse-level authorization and can be employed for persistent as well as on-demand or ad hoc granting of privileges. Session services are used to monitor the initiation, transition, and termination of activities. Audit services ensure that processes are monitored and that the relevant information is captured in a secure manner.

Effective services architecture identifies that the necessary information is available and ensures that the proper capabilities are provided. This should be accomplished in a manner that provides straightforward integration capabilities while reducing duplication, inconsistency, and the need for extensive development. Most importantly, the services should enhance adoption and flexibility while reducing the costs of integration and operation.

Although a large part of the effort being expended by the ISWG participants is toward internal challenges, the impetus for change is coming from external relationships. Identity services need to address legacy challenges while enabling interoperability with other organizations' solutions. Eliminating application and vendor dependencies, leveraging open source solutions and relevant standards, and focusing on demonstrated interoperability will help to achieve this. Over time, the consistent adoption of SOI will help to eliminate challenges and barriers, both for internal and external initiatives.

Trust models are as much a business challenge as a technical one. Limiting risk and protecting the interests of individual organizations is often the gating factor for trust; third-party hubs and communities of interest work out whenever the business case is compelling and risk to the organizations is manageable. This has been demonstrated in government, the financial services industry, and elsewhere. Establishing clear requirements and expectations and implementing successful business models will go a long way to address this challenge. For identity information, providing high-quality, properly vetted information that is well understood will be a good start.

Show Me the Money

Businesses exist to make money. For many of the participants, identity services are a means for facilitating business relationships. Streamlining IdM, instituting effective business interaction, and improving time to market for product offerings are fundamental opportunities for these organizations. For others, identity services represent a business opportunity in themselves.

So, what's the business need and opportunity? In today's connected environment, principals are ill prepared to fully represent and protect themselves. Identity theft and associated fraud incidents are rampant, and the situation will only get worse. The many gaps in identity verification—along with information compromises—make trusting identity assertions and managing business risk increasingly difficult. It is reasonable to expect that relationships, not attributes, will become the preferred currency for verification. This will expose significant implications for trust models based on relationships. The need is twofold: to help individuals protect themselves and to help businesses understand who they are dealing with.

The opportunity here is for identity providers to act on behalf of principals and businesses. Identity providers can bring benefits to both parties by insulating them from risk; for example, the inappropriate disclosure or exploitation of identity or financial information. Relationship expectations and boundaries can be more clearly articulated, and performance against these monitored and publicized. For the consumer, this helps to control what information is exchanged and for what purposes; for a business, the costs of identity vetting are managed and the risk of fraud reduced.

For the IdSP, this could follow a fee-for-service or a subscription model. Although the market is in its infancy, a number of firms have already started to offer their services, while others are examining the opportunity and how they can differentiate themselves. As awareness grows, organizations with existing relationships might leverage these to a new level. This opportunity represents a higher level of interest in identity services and will provide use cases and business justifications that clarify service capabilities.

Setting Boundaries

As in any model, it is important to establish boundaries, capabilities, and responsibilities for identity services. One of the basic objectives of the identity services model is to establish explicit boundaries or intersections where services interactions are appropriate. Figure 5 illustrates these boundaries. The current situation, as described by an ISWG participant, is a lack of recognition for these lines of demarcation when accessing identity information and related capabilities—in both commercial and internally developed applications.

The goal is that identity services should be delivered at either the domain or enterprise level. In principle, applications should interact with the container, containers should interact with the domain, and the domain should interact with the enterprise (the "Good" approach in Figure 5). In reality, these boundaries are not enforced, so that applications interact directly with other applications, domains, and enterprises (the "Bad" approach). This discipline must be recognized and enforced for internal environments and by the vendor community.

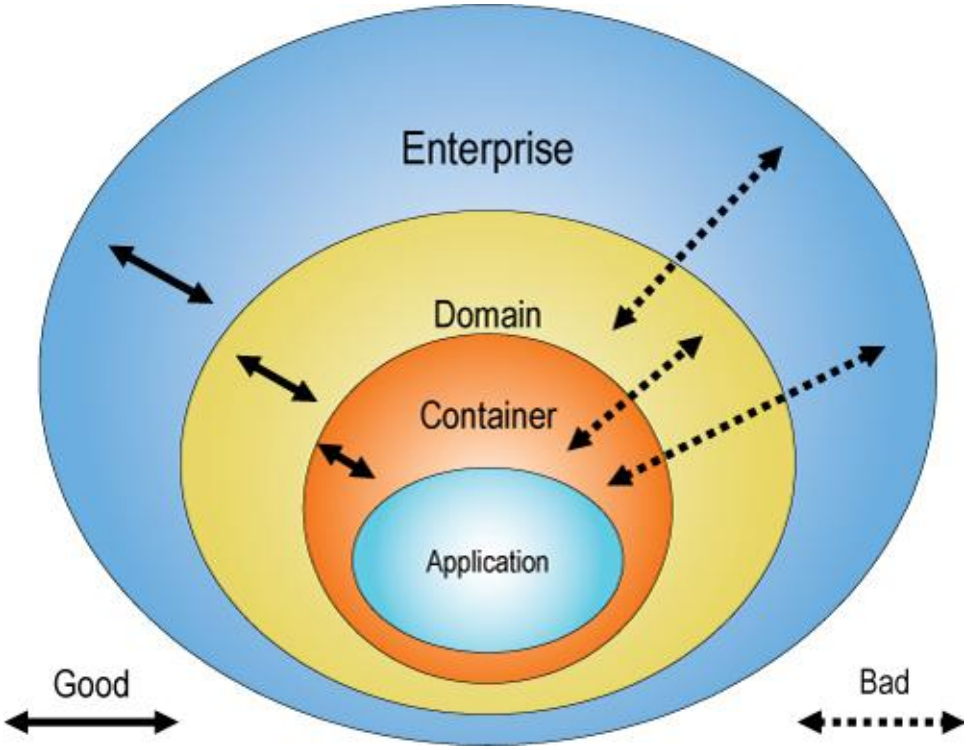

Figure 5: *Boundaries*

Conformance with these boundaries will enhance their adoption in broader situations. Figure 6 shows how identity information might be expressed between business entities, into communities of interest or brokering situations, and into loosely coupled business environments. It remains to be seen how moving from a specific to a more generalized situation will evolve, but the objective will be that the services remain consistent. Ultimately, identity services must share the same interfaces and specifications and provide consistent functionality to ensure interoperability.

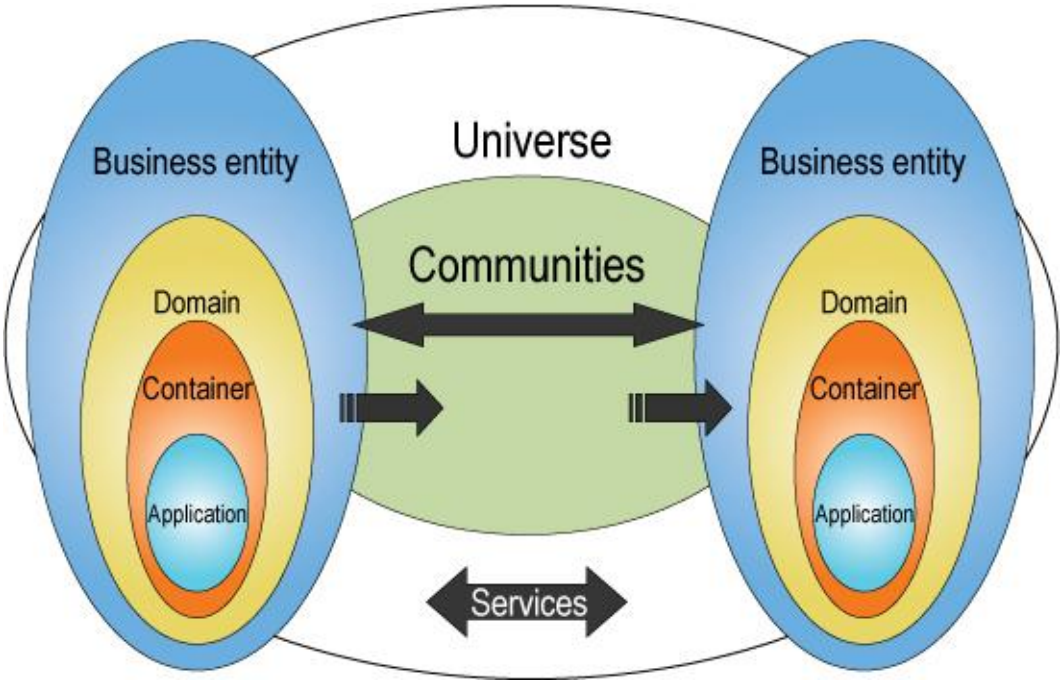

Figure 6: *Extending Services*

Conclusion

The opportunity to establish consistent and interoperable identity management (IdM) capabilities within and between organizations is compelling, particularly given the challenges and difficulties that organizations have experienced to date. While the vendor community has made progress toward internally consistent solutions, these are not keeping pace with the changing needs of businesses, customers, and society.

The IdM industry has an opportunity to reduce integration challenges and demonstrate value to customers by removing barriers to adoption and interoperability. Working with the Identity Services Work Group (ISWG) to promote consistent characteristics and interfaces can lead to broader understanding and cooperation and, ultimately, to more effective solutions.

Author Bio

Kevin Kampman

Senior Analyst

Emphasis: identity management, directories, provisioning, role management, identity services

Background: Kevin Kampman is a senior analyst for Burton Group Identity and Privacy Strategies. He covers identity and role management, directory services, provisioning, and electronic commerce. Prior to joining Burton Group, Kevin's duties included systems engineering, engineering management, integration and development, and project management with AT&T, Control Data Systems, Compaq/DEC, NCR, and TRW. From 1998 to 2007, Kevin managed Burton Group's Identity and Privacy, Security and Risk Management consulting teams in their interactions with enterprise customers. With over 20 years of experience, Kevin was a past chair of the Directory Services and Collaborative Computing Work Groups at the Automotive Industry Action Group (AIAG), a Michigan-based consortium of over 1,500 manufacturers. This work led him to being named two-time recipient of the AIAG Outstanding Achievement Award for contributions to the industry. He also co-authored All About Network Directories, published by John Wiley and Sons. Kevin is currently engaged with a international community of organizations chartered to develop a shared perspective on identity services.