Identity and Privacy Strategies

In-Depth Research Overview

Identity Services Architecture: Working Toward Consensus

Version: 1.0, Feb 02, 2009

AUTHOR(S):

Kevin Kampman
(kkampman@burtongroup.com)

Anne Thomas Manes
(amanes@burtongroup.com)

TECHNOLOGY THREAD:

Identity Management

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

Summary of Findings

Bottom Line: Agreeing on a standard way to satisfy the needs of all parties in a community is a difficult proposition. The Identity Management (IdM) market is no different. Given the variety of customer deployments and vendor capabilities, designing a consistent set of identity services usable by multiple user organizations is very, very hard.

Convincing vendors to develop products conforming to these services is possibly the most difficult challenge of all. The problems are not technical as much as they are conceptual, political, and economic. In light of this, the cooperation demonstrated in the Identity Services Work Group (ISWG) is an encouraging development.

Context: Today's IdM marketplace consists of suites and point solutions from a number of vendors. These were developed in response to specific customer requirements; some are burdened by the influence and overlap of vendor mergers and acquisitions. Customers are challenged to adapt their environment to vendor offerings, and frequently to bear the cost and effort of integration of other IdM solutions into their own environment. For the long term, this is undesirable.

The intent of an Identity Services approach is to bring reason to IdM by clearly articulating service boundaries, requirements, and capabilities. The benefits to customers are the ability to reduce or eliminate integration costs, to select the best-fit solution for their environment, and to align IdM capabilities with business requirements.

Takeaways: Today's IdM solutions have different heritages and were developed in response to different expectations:

- The business focus is on identity relationships.
- The technology focus is on process and procedures.
- The vendor focus is on product portfolios and point solutions.
    - The result of this is that these are expensive for customers to deploy and maintain; they lack flexibility and fail to meet objectives. To be successful, these three perspectives need to focus on shared outcomes.

Identity Services can offer a perspective to address these challenges, by:

- Leveraging the shared perspectives and understanding of both customers and vendors.
- Focusing attention on fundamental capabilities of IdM solutions.
- Providing consistent interfaces to these solutions.
- Reducing integration challenges and the associated deployment and maintenance costs

To develop Identity Services, these service-oriented principles provide guidance.

- “Separation of Concerns” provides a way to articulate legitimate points of abstraction.
- The “Façade” model provides a way to define services as a simplified interface to more complex processes.
- Patterns, or templates, provide a way to extend similar capabilities. This was useful in the case of authentication providers, which leverage credential collectors for different forms of authentication, such as smartcards and biometrics.

IdM is complex, and services definition is hard work.

- Designing a set of abstract, reusable services that supports business interactions based on identity information is exactly like designing the business that delivers that service: It requires a higher-level business perspective.
- Some of the complexity is self-imposed, by both the vendor and customer. This is a result of making IdM conform to the restrictions of complex and legacy applications and platforms; growth by acquisition.
- Defining services is an iterative and highly collaborative process.
- The outcome of the current ISWG effort is deceptively simple; it provides a high-level view of key capabilities along with one use case. The amount of effort that went into this was significant.

The ISWG's assessment of the effort so far is positive, but recognizes its limitations:

- The ISWG participants agree that the effort should continue under a more formal program to develop a more thorough architecture (i.e., more services) and additional use cases.
- It acknowledges the need to encourage broader customer participation.
- Additional vendor participation is also needed. Vendors can contribute by extending the work to a design and deployment initiative.
- The goal of that work would be to determine how to make the services real by developing migration and integration solutions, assessing standards contributions and gaps, and standardizing the effort.

Conclusion: Developing an identity services architecture has been productive; however, designing a comprehensive solution that satisfies the business needs of the consumer remains. Collaboration and analysis that contributes to a shared body of knowledge—as well as a common point of view— will foster successful outcomes.

To date, the Identity Services Work Group (ISWG) efforts demonstrate that a service-oriented perspective toward Identity Management (IdM) promotes a consistent, standard view of identity. However, accomplishing this on an industry scale requires a more formal program.

Analysis

Burton Group has been involved with the Identity Services Work Group (ISWG) since early 2007. This group of international organizations is establishing the requirements and architecture for a vendor-neutral approach to Identity Management (IdM). The goals and objectives of the ISWG are discussed in the *Identity and Privacy Strategies* overview "The Challenge of Identity Services." Prior to Burton Group's Catalyst North America Conference 2008 in San Diego, the ISWG consisted of customer organizations. As a result of recommendations made at Catalyst, participation was expanded to selected IdM vendors. This overview is intended to provide a broader range of experience and insight to the ISWG's analysis. The activities described in this overview represent the perspectives of both ISWG members and the selected vendors.

Identity Management: Where It's at, Where It's Headed

Establishing and characterizing an identity is more of a business challenge than an administrative task. Identity was once defined in terms of the relationship of a person to an organization. However, a single identity is no longer under the exclusive auspices of a single enterprise. Ownership of an identity is increasingly in question as user-centric initiatives gain traction. An enterprise can act as a representative for an identity in multiple relationships, thus providing additional credence to identity assertions.

As the scope and horizon for identity interactions broadens, traditional approaches to authentication and authorization are being challenged. How an organization establishes its relationships with individuals, and with other organizations, is changing. This evolution is forcing the IdM industry and its users to reexamine their assumptions about identity, the fabric in which identity operates, and the capabilities of the supporting infrastructure.

Starting in August 2008, the ISWG began focusing its attention on authentication and authorization services. These are the first in a long list of identity-related capabilities that the ISWG has identified for examination. The focus of the effort described in this overview was to describe a conceptual architecture for establishing identity and to explain how identity can be consumed for authorization purposes.

The Business Perspective

IdM is composed of a number of capabilities. These capabilities facilitate the management of a principal's relationship with an organization or to another entity. The business or top-level view of the identity lifecycle includes the creation, maintenance, and exchange of identity information. The perspective includes characterizing the relationship of the identity to the organization and the policies and context that govern the relationship. This translates into procedural activities such as registration, association and assignments, transfers, suspension, and termination.

The Technology Perspective

Beneath this business perspective, there is an administrative view of these capabilities. Here, IdM is described in terms of access controls, user and resource administration and provisioning, password and credential management, directories and repositories, roles, compliance, and audit. These administrative functions represent how technologists typically view and discuss IdM capabilities; these are the instantiations we need to address as we examine identity from a services perspective.

As an example, provisioning a user to a resource implies the creation of an account and access rights in a platform or application. This presumes that a digital identity or authoritative record has been created for the user and that sponsorship or approvals have been provided to authorize user access. This scenario is common to many administrative models.

An alternative situation is an access request made in real time. Here, assertions of relevant characteristics about the requestor are gathered and evaluated against access requirements. The user may be provided access by satisfying the requirement to act in a particular role.

The Vendor Perspective

Our perspectives of IdM frequently align to our organizational procedures. While these may be sufficient for today's environment, they may not provide the flexibility to adapt to more general or future challenges. Vendor capabilities have also evolved to include the contributions of acquisitions as well as to address specific customer project- or resource-based expectations and requirements. In at least one situation, a vendor solution emerged from a specific customer deployment, and was subsequently filtered through several acquisitions. For these reasons, one vendor's IdM capabilities rarely align directly with those from another. This means that when customers need to integrate solutions from multiple vendors, they assume the challenges and maintenance burdens that result from the different approaches.

The bottom line is that the effectiveness of today's IdM solutions is hampered by a number of factors. Today's solutions demonstrate limited perspectives arising from:

- The operational problems they were developed to solve
- Vendor and customer mergers and acquisitions
- Multi-vendor product overlaps and differences
- Absence of standards
- Tactical or user-developed applications that address specific customer challenges

Maximizing Flexibility: The Identity Services Model

A services model provides an alternative to satisfy the procedural, technical, and administrative requirements for a given task. However, what's important is that the services model provides an abstraction layer that masks the syntactic differences between vendor offerings and that can serve as a translator or value-added proxy to harmonize functionality across different implementations and to support interoperability between those implementations.

The key is to identify fundamental capabilities that can be organized and utilized in a flexible manner in response to specific situations. For example, the collection, verification, and exchange of attributes associated with a user or resource is basic and common to most identity-related activities. If vendors provide common and consistent interfaces to accomplish these tasks, then the customer's integration and maintenance burden is reduced or eliminated.

Arriving at a shared understanding of these common and consistent interface points is profoundly difficult. As described in the preceding three sections, businesspeople, technologists, and vendors bring differing points of view regarding what a specific capability, such as authentication, really is. When the ISWG set out to describe an authentication scenario, each vendor and customer participant contributed a different set of expectations. Our initial assumption that vendors would be able to contribute common use cases and requirements based on customer experiences proved false.

Breaking down the problem into component activities contributed to our understanding. One of the participants described this process as a return to the “first principles” of identity. A guiding principle for our effort was “separation of concerns”: the association of activities and information with specific capabilities. Another principle was to describe the “what” (what is needed), not the “how” (how to accomplish the “what”). The ISWG specifically avoided using standards as guidance for how to characterize problems, although prior standards work helped us to partition certain responsibilities.

However, our discovery process required significantly more time and effort than anticipated. After five teleconferences and two on-site meetings, the group finally arrived at a shared understanding for a logical architecture for one service: Authorization. A concrete architecture and a detailed design have yet to be completed. Our experience underscores the difficulty of arriving at an understanding of these fundamental capabilities. The work of standards bodies provided some guidance; evaluating the sufficiency of these efforts is a remaining activity.

Getting Back to Basics

Identity management continues to grow in features and capabilities, including role management, fine-grained authorization, and audit and compliance, at the same time that customers are asking for the essentials and interoperability. Like a weight loss program, addressing the intake and digestion of identity food (i.e., information) is core to the solution. Despite the promises of miracle solutions, there's no way to avoid addressing the fundamentals.

Since the ISWG and vendors began working jointly, the group has worked diligently to define the fundamental expectations for authentication and authorization because these are core capabilities of identity services. Going in, the participants all thought they understood what authentication and authorization were. They were surprised to learn otherwise.

What the ISWG discovered is that everyone involved brought a different perspective, and that the group needed to peel away the layers of interpretation. At their root, authentication and authorization services are really based on exchanges of information to satisfy conditions. The conditions to be satisfied are established in a context; the context describes the policies or conditions that must be satisfied. For example, to conduct simple authentication, an application will request, and the user will supply, a pre-established set of attributes such as a user name and password. Success (i.e., an authenticated user) results when there's a match of the supplied attributes to the values required by particular criteria. If the context policies permit, a new user may be permitted to register prior to providing authentication credentials.

This seems simple enough. Authorization isn't greatly different: For a user meeting a set of authentication criteria and satisfying contextual requirements (success), authorization to access resources will be granted. As stated previously, it comes down to the exchange of information that meets certain conditions. The industry has started to build up a vocabulary of new terms such as claims, assertions, and obligations to characterize this. The idea of context has come to the foreground as a way to characterize exchanges and interactions.

Technology consumers and providers have built up so many abstractions that obfuscate what's happening that it becomes difficult to see what is really necessary. At the same time, the ISWG realized that there's a need to describe conditions that, until now, have been assumed. As industry develops a more flexible model for identity activities, the need to characterize the business environment gains importance, particularly with regard to trust. Trust underscores many business activities. Making trust something that can be characterized and leveraged in an automated manner is still a challenge.

Staking a Claim

Our discussions so far have provided several key insights. First, authentication and authorization operations rely on the exchange of information and are more closely related than the ISWG participants originally thought. This information has a degree of confidence associated with it. The provision of supporting information results in a claim or validated assertion.

Identity capabilities take place in an environment, or context. Understanding the context enables the enumeration of policies that must be evaluated and satisfied for successful outcomes. Policy determines which assertions must be exchanged and the degree of verification or validation required. The ISWG's logical architecture relies on claims, policy, and context capabilities.

Looking at the fundamental building blocks, the ISWG realized that the industry may only require a simple set of capabilities to accomplish the bulk of identity-related operations. This is one of the key findings of the ISWG effort: The same fundamental identity-related activities are viewed in many different ways. These fundamental activities are the likely building blocks for future use cases.

Policy, Policy, Everywhere

Policy represents the set of rules or conditions that must be satisfied in order to provide access. Policy has several important dimensions: overall management, information, decisions, and enforcement. Respectively, the system components that consume and manage policy information are known as a Policy Administration Point (PAP) or Policy Management Authority (PMA), Policy Information Points (PIPs), Policy Decision Points (PDPs), and Policy Enforcement Points (PEPs). The interaction between the PDP and PEP is most important to this discussion: A PDP evaluates whether the conditions of a policy are satisfied, and the PEP grants or denies access according to the PDP decision. Although the PDP and PEP are frequently co-located, the logical distinction is important.

The abstraction of policy is helpful and has been formalized in the eXtensible Access Control Markup Language (XACML). However, policy is pervasive. It can be embedded and acted upon within a particular capability, such as an application or service. For example, an attribute service may form a request-response based on policies governing privacy. This partitioning indicates that policy is required to mediate between capabilities and acknowledges that multiple policy components interact with each other. As part of the ISWG's examination effort, the group determined that while a PEP is not itself a service, it is central to the interaction between an authorization and authentication service. A PEP may be located within an application, at an application container boundary, in the intermediary infrastructure (e.g., Web Service Gateway or Web Access Manager), or in support of an enterprise service (e.g., a policy server).

Everything Happens in Context

The context service identifies and enumerates the express policies (i.e., those that govern the interactions between external components) that must be enforced for a particular situation. Policy determines which claims (i.e., validated assertions, where assertions are attributes needed to satisfy policy) are required, and where these are sourced. The context service intermediates the exchange of policy and claims between the session, attribute, and resource services.

Capabilities: What's In, What's Out

There are a number of capabilities that compose or contribute to identity services. As the ISWG examined these capabilities, and particularly as the group sought to differentiate them from underlying protocol mechanisms, a categorization model emerged. Figure 1 identifies several distinct characteristics:

- **Producers and consumers:** These are the actors in a relationship; for example, the user and the application. The roles may reverse, for example, when an application provides a response to a user request.
- **Mediators:** Mediators facilitate the interaction between producers and consumers. A mediator may manage the collection of information from the authorization and the claim service and provide it to the authorization service or to the resource provider.
- **Collectors and transformers:** These assemble and package information from one or more sources in a form that is consumable by the requesting party.
- **Transports and protocols:** These provide the mechanisms to exchange information between distinct capabilities using standard interfaces.

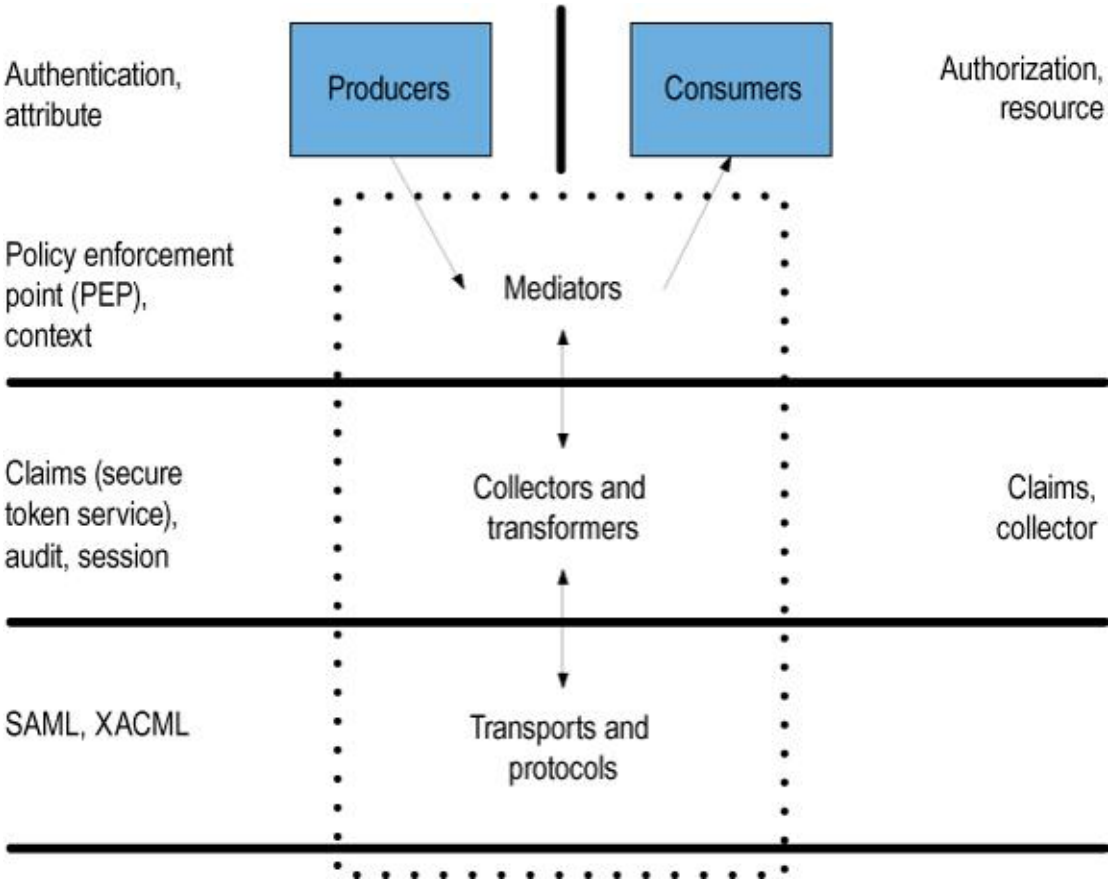

Figure 1: *Characteristics of Capabilities*

The following list represents the capabilities and components under consideration by the ISWG; it is broader than those established in the *Identity and Privacy Strategies* overview *"*The Challenge of Identity Services" and will continue to be refined as the ISWG continues its examination:

- **Audit service**: An audit service provides for the collection or logging of relevant activities as well as subsequent examination and reporting on those activities. Audit and logging are not specifically identity services but can participate in the process.
- **Assertion:** An assertion is the value of an attribute.
- **Attribute service:** Attributes describe the characteristics and properties of a principal. An attribute service provides authoritative information about a principal in accordance with policy. It may leverage a virtualization capability to associate information in multiple repositories to a single entity.
- **Authentication service:** Verifying a claimed identity is the responsibility of an authentication service. Specific methods of authentication may provide increasing levels of confidence. For example, two-factor authentication requires that the user present a physical token and supply a corresponding identification number. This is considered "stronger" than the presentation of a user name and password combination (reference the Liberty Alliance Identity Assurance Framework).
- **Authorization service:** An authorization service provides an authorization decision granting a requestor access based upon the satisfaction of authorization requirements associated with a resource (i.e., the requirements associated with a resource, as expressed in policy).
- **Credential collector:** A credential collector is a component of an authentication provider that requests a specific form of credential; for example, a smartcard or biometric token or one-time password (OTP).

- **Claim:** A claim is an attribute and assertion pair, expressed in the form Attribute=Assertion. An identity may "claim" that commonName=. A claim is evaluated by the recipient and evaluated according to policy.
- **Claims and security token services:** A security token service represents one possible implementation of a claims service. It is responsible for assembling and transforming claims, or assertions, into consumable formats. It conveys an assurance from the producer to the consumer. The consumer may choose to rely on the claim based on the combination of the assurance and a pre-existing trust relationship with the provider.
- **Context service:** The interactions between capabilities involve the exchange of attribute values and governing policies. Certain of these may not be interchangeable between capabilities, but do require interpretation and evaluation for the overall scenario. A context service manages the interactions between capabilities, particularly the attribute, session, and resource service.
- **Endpoint administration:** The lifecycle management of the relationship between a principal and an organization includes the management of attributes and associations. This capability facilitates the collection and management of this information.
- **Federation:** Federation is a higher-level capability that allows one domain to consume assurances (i.e., claims) produced by another domain, rather than relying on claims it generates itself. Capabilities that it enables include cross domain authentication and authorization.
- **Obligation:** An obligation is an operation that must be performed by a in order to enforce a policy decision. For example, creating an audit record could satisfy an accountability obligation.
- **Policy:** Policy represents the overarching and specific management and evaluation of rules within and between capabilities as discussed in the "Policy, Policy, Everywhere" section of this overview. Although policy is not a service in itself, a PEP may act as a mediator to coordinate interactions between capabilities.
- **Resource provider:** The resource provider manages and mediates access to the requested resource. The resource provider mediates for the actual resource, which may be either physical or logical in nature.
- **Resource service:** The resource service acts as a PIP for a resource. A resource service externalizes the policies and characteristics associated with a resource for authorization decisions. This distinction was established to distinguish between internal, resource-specific requirements and activities.
- **Roles:** Roles are an abstraction point that can characterize the principal (acting in or performing a role), and the capabilities provided by a resource (i.e., provided to a role). Roles reduce the identity coupling and administration burden for an application.Roles are typically represented as attributes and collections (i.e., membership).Roles may also be represented as a hierarchy that denotes role relationships (e.g., either Manager to Employee or Physician to Patient). Policies based on explicit roles help to simplify application maintenance and also to formalize role adoption.
- **Session service:** 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. It also maintains authentication, identity, and authorization context.
- **User interaction system:** This is the physical interface to the requestor. It may be a browser, terminal, or other device, such as a mobile phone.

The Façade for Identity Services

The purpose of a façade is to provide a simple interface to a more complex set of resources. As discussed in the *Application Platform Strategies* technical position "Application Factoring," a façade layer allows organizations to develop, scale, and evolve distributed application components, and to minimize the impact of changes on other components that invoke them.

If identity services are viewed as a set of simplified interfaces to a more complex set of capabilities and then implemented in this manner, the benefits to consuming applications become clear. An application developer can rely on a set of identity services to leverage identity information; the developer need only concentrate on the relationship of identity to the functions of the application. This reduces the complexity of the development process, improves flexibility, and simplifies the deployment, maintenance, and support requirements.

The ISWG developed a logical architecture for identity services based on the primary capabilities of authentication and authorization (see Figure 2). Authentication and authorization enable interaction between a requester or resource consumer and a resource provider (i.e., relying party). The Authentication Service and Authorization Service are supported by the foundational identity capabilities provided by the Claims or Secure Token Service, Context Service, and Attribute Service. Additionally, the architecture calls out the following related capabilities: the User Interaction System, Resource Provider, Resource Service, Session Service, and Audit Service. These capabilities are described in the "Capabilities: What's In, What's Out" section of this overview.

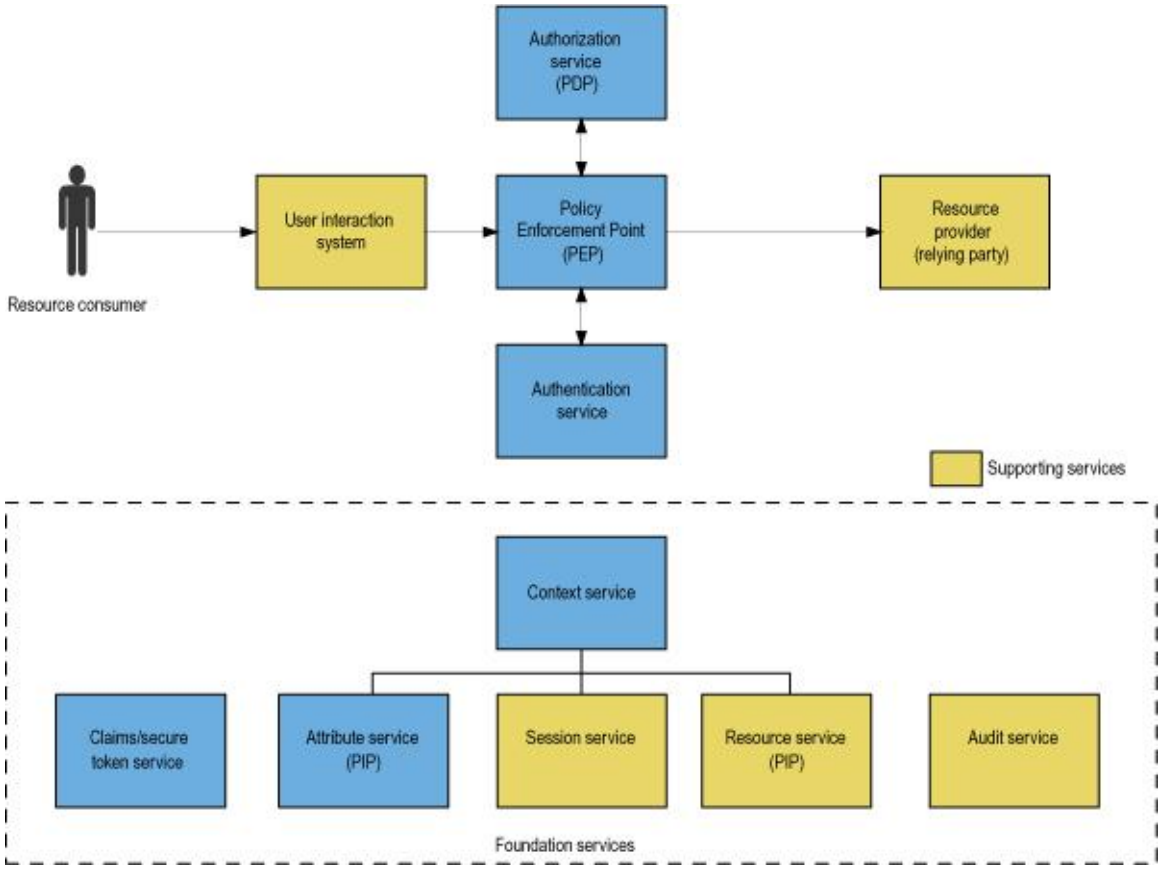

Figure 2: *Identity Services Logical Architecture*

First and foremost, identity services should enable us to understand who someone is. This is what we know as authentication. We want to know who someone is in order to allow them to do something; that's authorization. Authentication and authorization represent the entry point for identity services. Authentication and authorization are distinct yet interrelated; authentication is an obligation, or an operation performed in the context of authorization.

An identity exists in a context. This context consists of characteristics that are bounded by relationships and an environment. For example, the relationship of a customer to a financial institution is different than the relationship of a vendor to a bidder in an online auction. The rules governing the relationship, how transactions are conducted, and so on, are specific to the respective environments.

The characteristics and relationships associated with an identity are typically represented by attributes. Attributes reside in repositories, such as a directory or database, or are provided interactively. An attribute service provides a consistent mechanism to access attributes about an identity.

An assertion is a declaration by an authority that a subject is accurately described by (or "possesses") an attribute. Attributes demonstrate credibility based upon validation or certification of the information they contain. A claim is a validated or verified assertion about an identity. Claims are one of the currencies in identity exchanges.

Identity services depend upon additional capabilities in order to function effectively. While the authorization service depends upon the authentication service to provide proof of an identity, it does not invoke the authentication service directly. The authorization service invokes an intermediary or mediator, the PEP, to gather required information from the authentication service. The authorization PEP performs tasks on behalf of the authorization service, such as notification, verification, caching, and transformation of claims provided by the authentication service.

Getting at the Core: An Authentication Use Case

Once the group arrived at the shared understanding of the logical architecture depicted in Figure 2, the ISWG was able to work through the application of a specific customer problem. The participants chose the initial authentication that would take place at a portal, for example, for web-based single sign-on. The consensus view of the ISWG's discussions are described in the use case steps in Table 1, and depicted in Figure 3.

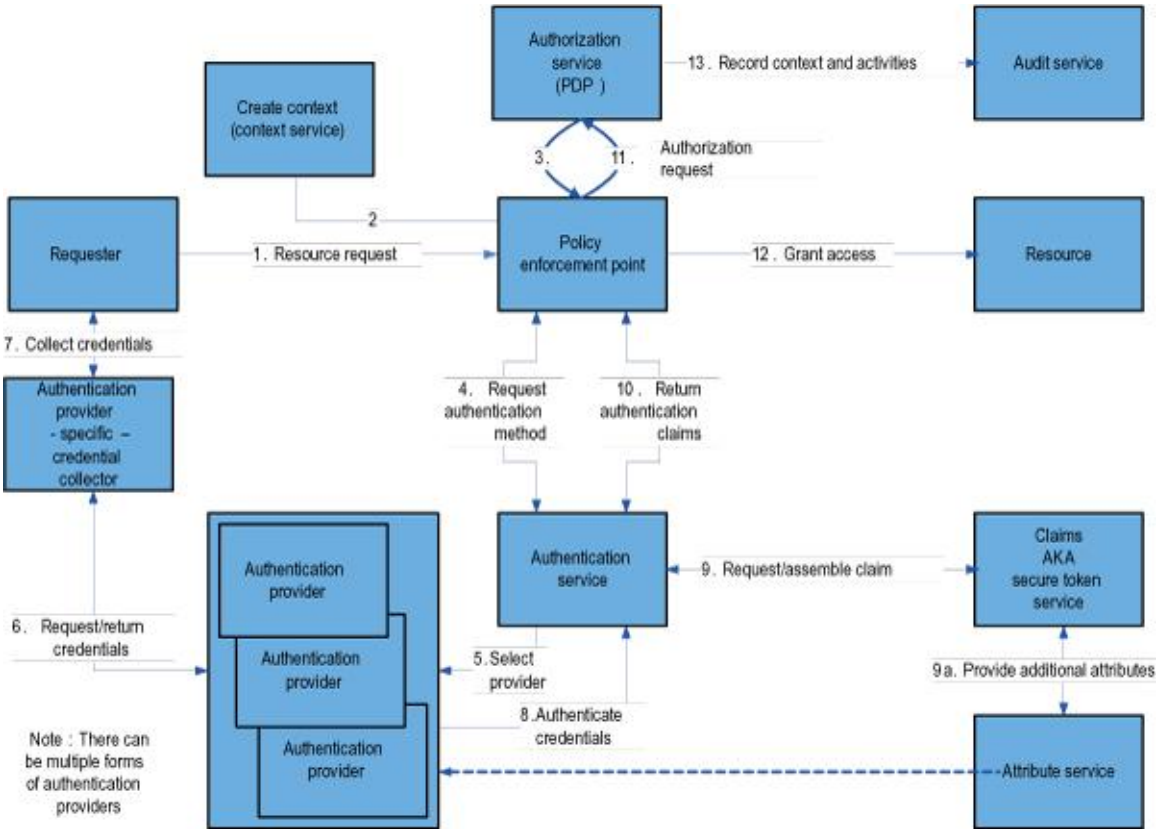

Figure 3: *Authentication Use Case*

Title	Authentication Use Case
1. Brief Description:	Initial authentication for Web Single Sign-On

2. Goal:	Accomplish authentication and provide access to requested resource
3. Actors:	Requestor, application (resource), responder
4. Pre-conditions:	Requestor has not been authenticated. Requestor has been provisioned to the resource. This is a new request for access.
5. Steps or flow:	1. Requestor interacts with a browser (User Interaction System) and requests a resource. The request is issued to the .2. A context is established based on conditions provided by the .3. The authorization service (i.e., PDP) determines that the resource is protected and requires authentication to take place.4. The authorization service requests the appropriate set of credentials (authentication method) from the authentication service (in this case via a browser redirect).5. The authentication service selects the appropriate authentication provider based on the policy articulated by the .6. The authentication provider invokes the corresponding credential collector.7. The credential collector solicits and returns the requested credentials to the authentication provider. It understands the method required and the information needed.8. The authentication provider returns the authentication credentials to the authentication service.9. The authentication service requests a claim from the secure token service (yielding validated authentication assertions).10. The authentication service provides the claims to the authorization service .11. The requests authorization by the authorization service PDP, based on the claims issued in step 10. Steps 3 and 11 are the same; the difference is that in step 3, the claims were absent or insufficient based on the policy.12. The provides access to the resource by sending it a validated set of claims in the token.13. The authorization service expresses the requests, decisions, and results to the audit service.Failure mode: In Steps 7, 9, and 11, insufficient authentication credentials could result in a repeat of the request for valid credentials, or in a denial of access to the requested resource.

Table 1: *Authentication Use Case*

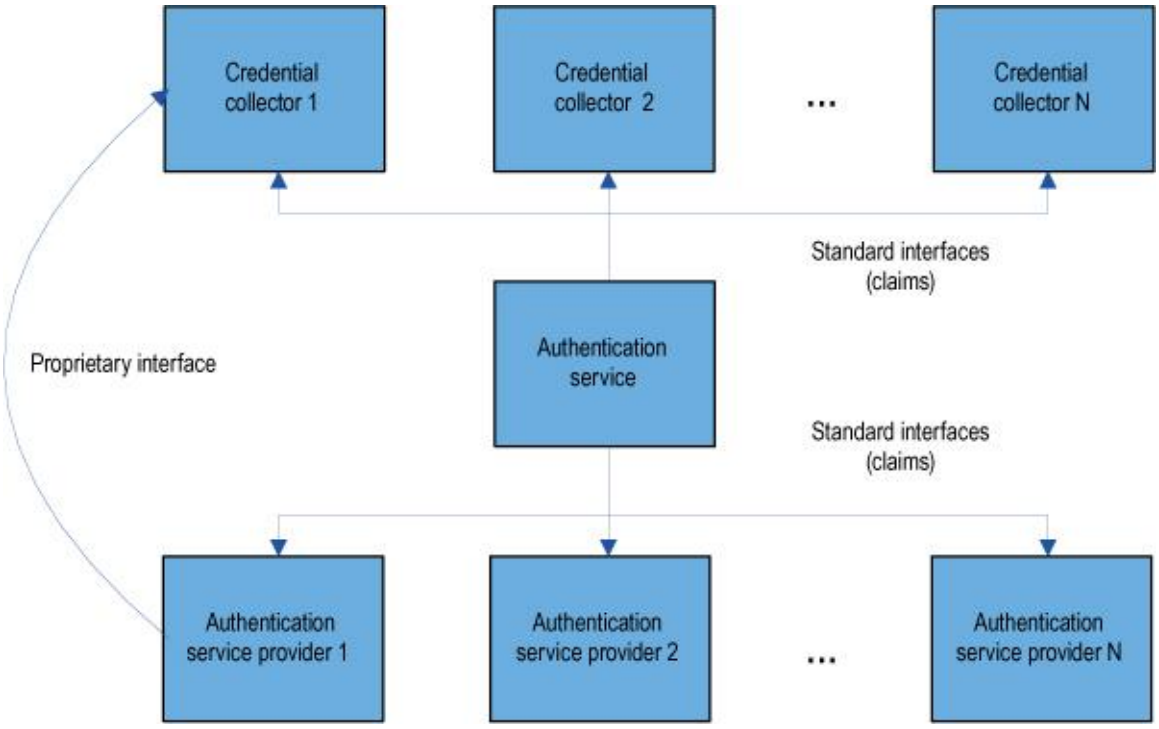

Figure 4: *Authentication Service Providers*

Authentication: Many Routes, One Destination

In the Authentication Use Case, the authentication service calls upon specific authentication providers and their corresponding credential collectors to gather the appropriate credentials from the requestor. The purpose of this distinction is to recognize the various mechanisms that may be employed to authenticate a user. For example, soliciting a username and password is much different than collecting a biometric of the user, a one-time password, or a digital signature. Each of these represents context-specific patterns (models or templates that exhibit a consistent set of behaviors).

As shown in Figure 4, this provides the authentication service the ability to deal with standard and proprietary collection mechanisms. An aspect of the logical model that is not immediately obvious but addresses a specific customer requirement is that a service from one vendor should be able to integrate with the service offerings from one or several other vendors. This provides customers with the flexibility to address special market needs and business models that a single vendor might not be able to address. For example, an institution may decide to leverage an outsourced service for consumer authentication or the capabilities of a federation provider.

Next Steps: Authorization

The authentication use case (see Figure 3) describes a high-level interaction with the authorization service. In reality, these are distinct yet highly interdependent capabilities. While the ISWG did not have the opportunity to examine authorization to the same extent as authentication, the ISWG recognizes the customer demand for a highly granular expression of application authorization leveraging the policy mechanisms described in this overview. This represents a future opportunity for analysis by the ISWG.

As the ISWG considered the implications of multiple forms of authentication, the variety of resources implicated by a resource service also came into consideration. The abstraction of an authentication provider and a credential collector may have a corresponding corollary with physical and logical resources. For example, authorizing access to a building by a Physical Access Control System (PACS) has similar implications to the collection of a biometric credential.

In the assumptions identified in the use case, the ISWG included the statement that the requestor had already been provisioned to the desired resource. This represents the characteristics of a stateful identity, one that is known and perhaps captured in an access control repository associated to or with the resource. As industry considers the opportunity to abstract identity, the idea of stateless identity assertions comes into play. This has already been demonstrated, for example, in Shibboleth, where asserting an association with an educational institution, rather than asserting a student name, is sufficient for authorization. This approach indicates the need for a more thoughtful examination of roles, relationships, and other forms of association, and their sufficiency for authorization decisions.

Recommendations

As an ad hoc initiative, the ISWG membership has expressed frustration with current IdM vendor offerings and the need for more consistent mechanisms to leverage identity capabilities. Working together, the group has exposed several conditions. First, there is not a clear, detailed, and consistent understanding of IdM capabilities among either customers or vendors. Each participant's perspectives and solutions are shaped around the adaptation of identity technology to particular business problems, and the manner in which vendor IdM portfolios are developed.

Standards address certain things well; they fall short on others. While the XACML model provided valuable insight into the distribution and complexity of policy and the environment in which identity is expressed and consumed, it does not provide a comprehensive perspective that addresses the responsibilities and interactions of other service components. XACML is a policy language, not a service abstraction. This is not an indictment of the good work that goes into standards efforts, only an observation that they leave work to be done. There is as much of a last mile of interpretation for standards as for product integration.

The ISWG indicated that applying service oriented architecture (SOA) principles to the identity problem was beneficial. Exposing the fundamentals of information exchange, production, consumption, and transformation demonstrates that analyzing identity operations for basic functionality can contribute to simplicity and reusability. Separation of concerns helps to keep these operations lean, understandable, and effective.

Some of the complexity of IdM may be self-imposed. The ISWG learned that breaking the problem down is difficult. It is time consuming and requires commitment. The value of working together as a group was that the multiple perspectives of the contributors helped the ISWG to arrive at a meaningful understanding of the problem and how to move forward, but much work still remains.

To succeed, the ISWG and its efforts must be formalized. The ISWG needs continued investment and commitment by both vendors and customers to produce, implement, and deploy a comprehensive architecture. This would establish work efforts and help to solicit the contribution of time and money. At a minimum, a formal ISWG effort is probably a half-time activity for a sizeable body of architects, in order to produce a viable architecture. That's just the start; vendors will then need to implement the architecture and test it for interoperability.

Another guiding principle for this effort was to focus on progress, not perfection. The architecture model and associated use case set forth in this overview represent a useful perspective of identity services. It is sufficiently simple to demonstrate the viability of the approach, yet broad enough to apply to a wide range of requirements. As a next step, the ISWG participants should determine if the work thus far is sufficient to demonstrate a working model of the approach.

Customers should recognize that until there is a shared understanding of the services model, and products designed to satisfy it, there will not be seamless interoperability. In the near term, it is realistic for companies to expect that one vendor's approach to identity service will align to their own approach. This leaves open the opportunity for integration vendors to bring customer requirements and other vendor solutions together.

Conclusion

Developing an identity services architecture has been productive; however, designing a comprehensive solution that satisfies the business needs of the consumer remains. Collaboration and analysis that contributes to a shared body of knowledge—as well as a common point of view— will foster successful outcomes.

To date, the Identity Services Work Group (ISWG) efforts demonstrate that a service-oriented perspective toward Identity Management (IdM) promotes a consistent, standard view of identity. However, accomplishing this on an industry scale requires a more formal program.

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.

Copyright 2009 Burton Group. ISSN 1048-4620. All rights reserved. All product, technology and service names are trademarks or service marks of their respected owners. See Terms of Use and publishing information at http://www.burtongroup.com/AboutUs/TermsOfUse.aspx