White Paper

The Identity & Access Management (R)evolution

Federation and Attribute Based Access Control

AXIOMATICS
A New Perspective on Identity & Access Management

Executive Summary

Identity & Access Management (IAM) refers to the combination of governance procedures and technology that enables organizations to meet a broad set of requirements regarding regulatory compliance and the integrity, confidentiality and availability of information.¹

Over the years, IAM has evolved into an increasingly important and complex segment within IT infrastructures. Large organizations maintain administrative IAM functions which consume considerable technology investments, operational costs and professional services. IAM thus also represents a considerable burden on IT budgets.

Requirements are however rapidly changing. Where existing IAM technologies and procedures focus on abilities to restrict access, organizations are more challenged with the need to share information and to collaborate across organizational borders in a secure manner. Where existing IAM infrastructures offer a static and coarse-grained set of access configurations, business processes demand a more dynamic and fine-grained approach. Capabilities to speed-up deployment of new services are also needed.

As a result, many organizations are currently striving to develop new strategies in their IAM vision and roadmap planning. While investments made need to be leveraged, organizations look for IAM capabilities that will make them more agile and responsive to change requests.

This paper discusses these changing requirements and suggests that the necessary IAM evolution can be achieved with two important new concepts that combined amount to what could be considered a small IAM revolution: the combination of Federated Identity Management and Attribute Based Access Control (ABAC).

The findings show that mature methodologies, standards and technologies are available with which IAM investments made in the past can be leveraged while new demands for simplified administration and information sharing and related fine-grained access controls can be met. These new IAM concepts even bear the promise of considerably reduced operational costs, since a number of tasks today handled in separate IAM governance processes can be embedded and delegated to existing business processes.

Changing requirements

Current Identity & Access Management (IAM) infrastructures are typically aligned with requirements gathered when the need for a separate IAM infrastructure first was conceptualized. Today, these requirements tend to be obsolete or inadequately defined in relation to actual needs.

The quotations listed in Table 1 below are from two different IAM related requirements specifications from the years 1999 and 2009 respectively:

<table>
<thead>
<tr>
<th>IAM RFI 1999</th>
<th>IAM RFI 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Protecting business critical assets against unauthorized use through strict enforcement of need-to-know level access controls.”</td>
<td>“Support a shift from a ‘need-to-know’ paradigm to one of ‘need-to-share’. This shift increases the need for standards, methodologies, and technologies to balance the ability to protect information and the ability to share that information with those that need it most, while maintaining the privacy rights of individuals. Traditional access management paradigms are inadequate for meeting this need.”</td>
</tr>
</tbody>
</table>

Table 1: IAM-related requirements specifications, 10 years apart

These documents reflect a typical shift in perspective from the “need-to-know paradigm” to one based on the “need-to-share”.

¹ Some years ago a Gartner report with the title “Consider Identity and Access Management as a Process, Not a Technology” gained considerable attention with its emphasis of the procedural aspects (Gartner Research, ID Number: G00129998, September 2005). It made an important point by balancing the notion that technologies somehow can automate compliance and governance by means of pure magic, an impression technology vendors sometimes may seem to convey.
While access control policies in the past often were based on the ambition to derive a need-to-know level from the job tasks an individual had been assigned, information security practitioners today may emphasize the risks that arise if restrictions are too inflexible and the IAM bureaucracy itself hinders the necessary information flow. In an emergency, the availability of information may be crucial and the risks introduced by obstacles hindering fast and efficient information sharing can be unacceptable from a business continuity perspective.

At the same time, requirements due to regulatory compliance which calls for efficiency and effectiveness in internal controls put an emphasis on more fine-grained access controls. “Recent compliance demands for more granular access control and policy transparency have increased urgency to adopt an architectural model where authorization and entitlement management are consumed as a service rather than embedded within business applications.”

### Shifting Perspectives

The requirements referred to in Table 1 illustrated the shift in perspectives that many organizations have been confronted with in recent years. It can be summarized as follows:

<table>
<thead>
<tr>
<th>FROM</th>
<th>TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall focus: To LIMIT and RESTRICT access aligned with need-to-know principles.</td>
<td>Overall focus: To COLLABORATE and to SHARE information aligned with need-to-share principles.</td>
</tr>
<tr>
<td>Focus on how to CLOSE DOWN systems, to limit and restrict access to include already known, identified and authorized users only.</td>
<td>Focus on how to OPEN systems for new, possibly even in advance unknown users, and for new types of information sharing, while ensuring strict compliance with privacy and confidentiality requirements.</td>
</tr>
<tr>
<td>Striving to CENTRALIZE administration of users and user privileges within an organization’s domain.</td>
<td>Striving to DELEGATE administration of identities and user privileges to owners of processes, data and related user populations as needed across organizational borders and domains.</td>
</tr>
<tr>
<td>Establishing a layer of SEPARATE PROCESSES for IAM governance.</td>
<td>Establishing IAM governance as a series of activities and controls EMBEDDED within existing BUSINESS PROCESSES.</td>
</tr>
</tbody>
</table>

**Table 2: Shifting perspectives**

### A Global Scope

This shift in perspective reflects the fact that organizational borders no longer constitute a relevant definition of the IAM scope

- **Users** have become mobile and access data from many different entry points. User populations can rarely be categorized as “internal” or “external”. Services are increasingly being made available to a larger audience via the Internet and data is presented in new contexts.
- **Applications** used for data processing may be hosted internally, by third-party service providers or accessed in private or public clouds.
- **Data** may be stored locally or in data centers located on the other side of the globe via dedicated data storage services.

This global IAM scope has very little in common with the situation of previous decades where corporate firewalls marked an outer and preferably impermeable limit of the IAM domain. In previous IAM infrastructures an inventory of users and their information assets could be established in advance. Principally, access control could be thought of as a combinatory matrix mapping users to the information assets within scope of their respective “need-to-know” levels. Consequently, centralized identity

---

2 “Entitlement Management: Ready to Enter the IdM Mainstream”, Burton Group, Dec 16, 2008
management, user provisioning and role management, the key element of most IAM infrastructures today, support the processes needed for maintenance of such an access matrix.

In today’s global scope, by contrast, neither users nor information assets are necessarily known in advance. The concept of a statically maintained access matrix fails. Access controls must match dynamically changing conditions and needs. Furthermore, in the new global IAM scope which organizations increasingly have to cope with, centralizing administrative burdens may violate ownership principles and raise a number of issues: If multiple organizations collaborate via shared information systems hosted by a third party, who should be the custodian and who should be the maintainer of user identities and access configurations? When eGovernment services are made available to the general public, how should privacy concerns and the mere size of user populations be managed and by whom? When service providers offer means for multiple stakeholders to create new types of information assets for mutual sharing, how can suitable access control capabilities be made available to the respective data owners?

The Next Generation IAM Capabilities

In response to questions such as those mentioned above, basic concepts of IAM infrastructures must be redefined.

- **User administration – the process of maintaining user identities:** Centralized repositories for user identities and related governance processes for the creation, alteration and termination of accounts must be adapted to the larger context of information sharing across organizational borders. Rather than operating one monolithic identity management solution for an ever-growing domain, organizations need to establish an association of trusted authorities in which user identities are managed locally by their respective authorized owners but made valid beyond, in domains or entities to whom a trust relation has been established.

- **Authentication of users – the process of verifying user identities.** Rather than having individual information systems handle authentication procedures themselves, authentication services need to be deployed servicing multiple information systems and cross-domain scenarios based on trust relations.

- **Authorization – the process of determining what a user, once logged in, is allowed to do.** Definitions of user privileges, whether achieved via intricate group or role assignments or through direct Access Control Lists (ACL), need to be replaced with a higher level of abstraction and logic. Rather than even trying to maintain static and pre-defined sets of permissions, the next generation IAM must offer generally applicable policies based on which access controls can be enforced dynamically at run-time. And rather than having each application or service implementing its own unique method for authorization, authorization schemes need to be standardized and externalized from individual applications.

**Federation and Attribute-Based Access Control (ABAC)**

In technical terms the above IAM feature requirements correspond to a combination of two important new technology trends and sets of standards:

- **Federated Identity Management** is typically utilizing the Security Assertion Markup Language, SAML.

- **Attribute Based Access Control** is typically based on the eXtended Access Control Markup Language, XACML.

The two standards SAML and XACML have been developed by OASIS in parallel and are well aligned.

**Federated Identity Management**

Federated Identity Management is a term used to describe a service oriented approach to identity management whereby functional services and identity services are separated:
Service Providers
Applications or content providers used for data processing can be seen as service providers. They provide their functional services to users of whom they do not need to know anything in advance, as long as they have been authenticated by an authority which the service provider trusts.

Identity Providers
These are services used to authenticate, verify and manage identities of users. Once a user has been authenticated, the identity provider issues a “token” (typically SAML based) which will be accepted as a valid identifier by service providers who trust the identity provider.

Figure 1: Federation
Federation capabilities represent a proven technology offered as components within all the big IAM suites as well as through various point solutions. Gartner’s annual Hype Cycle for Identity and Access Management placed federation as a mature technology on the “slope of enlightenment” as of 2006. The 2009 edition concludes that organizations also chose federation internally. “Federation also offers benefits when deployed internally by enterprises made up of multiple units that have historically managed their own users, and for which centralized user management hasn’t been feasible — technically or politically.”

Advantages with identity federation are well aligned with the new requirements outlined in Table 2.

- Identity management is delegated to a dedicated unit or to the authorized “owner”. Organizations will no longer have to manage “external” users.
- Collaboration between entities is simplified – adding new services to the community of trust is simple.
- Deployment of full-fledged services re-using an already existing infrastructure for authentication is fast and smooth – thus it is easy to “open up” systems for new user populations and purposes.

In addition federated identities offer other important advantages such as:

- Single sign-on between multiple applications / services.
- Simple upgrade paths for stronger authentication – moving from user name/password towards strong authentication for instance with smart cards only impacts the authentication service whereas service providers remain unaffected.

---

Attribute Based Access Control (ABAC)

While federation simplifies identity management and shared authentication within and across domains, it does not affect authorization – the process of determining what a given user is allowed to do within an application or service. Authorization has so far been built into the application logic of the software.

ABAC introduces authorization as an application-external and standardized service much the same way authentication services already have been externalized from applications.

ABAC makes use of the XACML standard which provides

- **A general request/response language** for authorization questions. Example: user Joe who happens to be an account manager in the Western sales region wants to review registered sales opportunities for East Corp., a customer in the corporate CRM system. This action can be captured in a rich XACML request describing
  - the **subject** (ID: Joe, role: account manager, district: western region, etc.)
  - the **action** (read)
  - the **resource** (account: East Corp., details: opportunity list, district: eastern region, etc.)
  - the **environment** (time of day, day of week, authentication strength, login location, etc)

- **A general policy language** which allows administrators to capture and author corporate policies in an exact language that enables secure evaluation of XACML access requests. Example: a policy may state conditions for access in the CRM mandating that read access should be granted if
  - The user has an account manager or a higher ranking role within the sales organization
  - The user’s district equals the district of the resource being accessed
  - The request is made during normal working hours via a securely encrypted channel

With a policy like this, the request in the above example would not be granted since the district of the user and the district of the resource (the customer’s account) differs.

- **A reference architecture** introducing
  - **Policy Decision Point (PDP)**, the service that receives XACML requests and evaluates them against XACML policies to determine whether access should be granted or not.
  - **Policy Administration Point (PAP)**, the administrative interface used to author and verify policies before they are put in production by being deployed to a PDP.
  - **Policy Enforcement Points (PEP)** intercepting access requests in or in front of applications. The PEP translates requests to XACML and sends them to the PDP.
  - **Policy Information Points (PIP)** are typically LDAP or services or other repositories holding attribute information about **subjects** and **resources**.

The XACML standard on which the Attribute Based Access Control concept relies is younger than the SAML standard used for Federation. The OASIS XACML Technical Committee has agreed on its Committee Standard for version 3.0 and a final approval of the new version can be anticipated in a very near future.

XACML has however been mature and production ready as of the 2.0 version released in 2005 even if the 3.0 version adds delegation of policy administration which is an important addition from a governance perspective.

The 2009 Gartner report “Adaptive Access Control Emerges” was still a bit indecisive in answering the rhetorical question: “Have we arrived at adaptive access control yet?” Since then, reality seems to have delivered sufficient proof – Axiomatics is delivering an adaptive authorization solution designed to handle hundreds of millions of users which may be seen as an affirmative answer. Yet, while SAML based

---

technologies already are commonplace commodities, XACML implementations have not yet reached the same level of market penetration.

Figure 2: Attribute Based Access Control / XACML reference architecture

Advantages with Attribute Based Access Control are well aligned with the new requirements listed in Table 2:

- Abstract and generally applicable policies replace static mappings between users and information assets. Evaluation of access requests is dynamic and executes in real-time which makes it easier to open up systems for new users and new use case scenarios.

- Policy-based access controls use descriptive attributes of the subject, action, resource and environment of an access request to define conditions for approval or denial of the request. Thus neither users nor information assets need to be known in advance which makes it easier to collaborate and to share information across organizational borders.

- Attributes used for policy decisions are typically maintained in already existing business processes. Privilege-giving attributes can for instance be data about users maintained in an HR system, roles defined in a business application, meta data describing a document in a document management system, a flag defining the state of a project in a project management system, a set of descriptive attributes defining the version and capabilities of a product in a Product Data Management system etc. etc. Management of privilege-giving attributes can thus be delegated and embedded in already existing business processes.

In addition ABAC offers other important advantages such as:

- Agile componentization by means of offering authorization as a service

- Simplified and cost-efficient deployment of new services since application developers, integrators and IT managers no longer have to bother about authorization algorithms and varying configuration schemes.
- Flexible enforcement of corporate policy compliance since PEP modules can be implemented on many different levels within the infrastructure: within individual applications, in web portals or gateways, within an enterprise service bus etc.
- The ability to offer fine-grained authorization capabilities since there, in reality, is no limit to the types of attributes that can be included in policy decisions.
- Sustainability since policies can be altered independently of the business logic of affected applications.
- Improved governance since business managers and auditors from a central point can verify the effectiveness and efficiency of access controls and their compliance with corporate policies.

**Federation and ABAC combined**

The SAML token typically issued by the authentication service in a federated environment contains important information about the user. The SAML and XACML standards are well aligned to enable smooth integration.

User attributes passed from the trusted authentication service via SAML can thus easily be parsed by the Policy Enforcement Point of an ABAC implementation and reused in XACML requests.

The following chain of events illustrates how the authentication and authorization services interact to achieve externalized authentication and authorization for a service provider:

1. User connects to desired service (through a client application or browser interface).
2. Service provider redirects the user to the authentication service.
3. User authenticates with the authentication service and receives a SAML token.
4. User is again redirected to the desired service provider.
5. Service provider accepts the user’s SAML token and grants access to the service.
6. Service provider’s XACML PEP intercepts the user request and translates the request to an XACML authorization request sent to the PDP whereby all the attributes of the SAML token are included together with information that describe the requested resource and the context in which the request is being made.
7. The PDP evaluates the user request against XACML policies and responds with a “permit” or “deny”. If attributes in addition to the ones contained in the request are needed for evaluation, the PDP may connect to the PIP.
8. The PEP grants or refuses access based on the PDP response.

**Leveraging Investments Made**

Combined, these technologies efficiently make use of already existing IAM infrastructures in which centralized identity management and corporate directories for attribute management already have been deployed.

Categories applied to organize directory information about users and resources such as user roles and groups, information and application classifications etc., can often be reused as trusted privilege-giving attributes in an ABAC deployment.
The figure below illustrates how governance procedures commonly are defined today:

**Figure 3: IAM overview – common procedures in existing infrastructures**

User IDs are requested by authorized requestors for different types of “internal” or “external” users. The request needs to be approved by an authorized approver before it will be implemented. Implementation typically means that account data and user profile parameters are provisioned to target systems. Finally, an audit log allows auditors and system owners to monitor all of the steps involved in the creation, alteration and termination of user privileges.

Full-blown, the next generation IAM will simplify these IAM meta processes. In the next generation IAM landscape, some important parts will change as illustrated below:

**Figure 4: IAM Overview – impacts of the Federation / ABAC evolution**
Authentication services are consumed using federation via trusted sources so there will be no need to manage “external” users.

With ABAC used for authorization in applications, there will be no need to deploy user profile data by means of user provisioning to target applications.

If management of privilege-giving attributes efficiently can be embedded in existing business processes, the administrative burden of separate IAM approval procedures will be limited.

While some of the quite elaborate governance procedures that characterize IAM implementations today can be simplified, new governance procedures may also be needed. Maintenance of privilege-giving attributes as an activity embedded within existing business processes may for instance impact and alter the business process itself.

However, in general the new IAM landscape can be expected to make organizations more agile and able to adapt to changing requirements.

Conclusions

Many organizations look for ways to refine their IAM processes and technology solutions to enable more efficient information sharing within or across organizational borders. Existing static and pre-defined access configurations make it difficult to achieve these goals.

Federated Identity Management combined with Attribute Based Access Control (ABAC) enable organizations to build their next generation IAM infrastructure while efficiently leveraging IAM investments already made.

In the past, information security requirements have often been seen as obstacles that make deployment of new services difficult or costly to achieve. By simplifying deployment of new information sharing services, the next generation IAM infrastructures contrarily will help organizations to benefit from new opportunities more rapidly. The new IAM infrastructure also removes the need for application developers to maintain authentication and authorization capabilities within their software, which lowers overall implementation costs.

Management of user identities and related user profile details can efficiently be delegated to the respective owner of that information. Entities will no longer have to manage the identities of “external” users.

Management of privilege-giving attributes can be embedded in existing business processes which will make organizations more agile and less dependent on a costly layer of IAM bureaucracy. At the same time their ability to become compliant with corporate policies and governance regimes is strengthened.