The Emerging Infrastructure for Identity and Access Management

Open Group In3 Conference
January 23, 2002
Jamie Lewis, CEO and Research Chair,
jlewis@burtongroup.com
www.burtongroup.com
Identity and Access Management

Strategic context: The virtual enterprise network
Identity and Access Management

The infrastructure challenge

• The disappearing perimeter turns enterprises inside out
  – Necessitates “opening” the network, creating a dichotomy: more flexible access and stronger security
  – Security must span logical and physical boundaries
  – Apps, databases, OS lack scalable, holistic means to manage identity, credentials, policy across these boundaries
  – Wireless and other devices increase complexity
  – Mistaken desire for “SSO” muddies the water
  – Inevitable intersection of public, private identity structures complicates an already complicated issue

• Legal, social, and regulatory trends raising the bar for protecting networks, identities, brands, and content
Identity and Access Management

The goal: creating context

- Business policy: liability, assurance for transactions
- Applications and services: access control and authorization
- Presentation/Personalization: What the user sees
- Authenticated Identity
  (person, application, group, organization)
- Defining relationships through quality of experience
- Relationships between identities and information
- Relationships between people, groups, and organizations
Identity and Access Management

The challenge: Interoperability and portability

Tightly-coupled, Persistent interior

Loosely-coupled, Dynamic exterior

Internal Systems & Data

Extranets

The Internet

Employees

Partner or xSP

Customers

Less-known

Unknown

THE BURTON GROUP
Driving Network Evolution
Identity and Access Management

The answer: Flexible infrastructure

Integration Internally

Federation Externally

Internal Systems & Data

Extranets

The Internet

Employees Partner or xSP Customers Less-known Unknown

Driving Network Evolution
Identity and Access Management

Bottom line analysis

• Identity and access management isn’t a “system”
  ➢ It must become a pervasive and federated infrastructure
  ➢ Centralized and decentralized, internal and external
  ➢ But we’re a long way from that pervasive infrastructure
  ➢ Standards are only just emerging, don’t address all needs

• Vendors are creating integrated product suites
  ➢ Niches remain for innovative standalone products
  ➢ But suites and products must become part of a broader, policy-based enterprise security solution
  ➢ Enterprises solutions must integrate with the world at large

• Enterprises should develop an identity and access management architecture and migration strategy
Identity and Access Management

Agenda

• Business drivers
• Architecture
• Interoperability and portability
Identity and Access Management

Agenda

• Business drivers
• Architecture
• Interoperability and portability
Business Drivers

Opportunities and requirements

• Internally: Lower costs, improve productivity
• Intranet and extranet access to apps; improve value chain efficiency; improve customer service
• Enterprises working to leverage assets—brand, customer base, market presence—to grow, become more efficient
• Meet regulatory requirements: Privacy
  ➢ Lightning rod issue motivating regulations ("opt-out rights")
  ➢ Uneasy balance between personalization and privacy
  ➢ European Data Protection Act creating urgency
• Industries with steep requirements:
  ➢ Petroleum (secure communications across the world), legal services, insurance, manufacturing…
Business Drivers

Opportunities and requirements

• Pharmaceuticals and health services
  ➢ Clinical trials involving patients, doctors, health care professionals; research with partners, universities
  ➢ FDA regulation 21CFR11 requires “signed” electronic records, “validated” development systems; audits, fines
  ➢ Health Insurance Portability and Accountability Act (HIPAA) requires confidentiality of records

• Financial services: consumer, biz-to-bank; bank-to-bank
  ➢ Many laws on banking secrecy, consumer protection
  ➢ Gramm-Leach-Bliley Act, protects the privacy of personal information that financial institutions share with third parties
  ➢ Corporate policies regarding disclosure of consumer info
  ➢ Enforcement by SEC, FTC, other regulatory agencies
Business Drivers

Benefits

- Identity and access management infrastructure enables secure business, enhances intranet security
  - Reduce risk of improper use of IT systems
  - Reduce risk of privacy or other regulatory violations
  - Save money by reducing redundant security admin
  - Accelerate time to market, reduce deployment costs by using general-purpose infrastructure to enable re-use
  - Competitive advantage with new services providing improved quality of experience (QoE) for customers

Bottom line: As an industry best practice, enterprises should develop an identity and access management strategy as soon as possible
Identity and Access Management

Agenda

• Business drivers
• Architecture
• Interoperability and portability
A layered VEN security architecture is emerging.
Architecture

Identity and access management solutions

• There’s no silver bullet, but infrastructure is emerging
  ➢ Directory services maturing, focus moving to directory-enabled services for I&AM, XML-based registries
  ➢ Identity management systems extending directories
  ➢ Provisioning systems taking on important role in bridging the gap between portals and enterprise security systems
  ➢ Web-based access management systems becoming a popular solution for centralized policy management
  ➢ Portals (personalization) becoming preferred interface to web-based resources

• Combination forms I&AM infrastructure
  ➢ Other components, including CRM and ERP apps, play important roles for overall relationship management
Architecture

Directory services

• Foundation for identity and access management
  - Primarily an identity and resource repository: people, organizations, groups, roles, and other resources
  - Authentication based on identity in directory
  - Personalization based on user attributes
  - Authorization based on user attributes (roles, groups)
  - Sometimes used as policy and certificate repository

• Enterprises are consolidating directory infrastructure
  - LDAP products have reached feature, commodity plateau
  - What’s next? XML protocols, multiprotocol servers, registries
  - But if it quacks like a duck . . .
Architecture

Provisioning systems

• Extend directory with tools to create, modify, or terminate user and app access to resources automatically
  ➢ Enable new users quickly (minutes, not days or weeks)
  ➢ Reduce admin costs and enhance security by automating account creation, termination across multiple apps
  ➢ Self-service, centralized password reset/synchronization
  ➢ Uses workflow for conditional processes
  ➢ Centralized policy mgmt: push roles, groups, privileges down to end systems

• Some organizations have rolled their own, but packaged software (directory-enabled) has arrived
  ➢ Expect convergence of provisioning and meta-directory
Architecture

Identity management

• Extends directory with tools for creation and maintenance of identity, including, credentials, entitlements, attributes
  ➢ Centralized user admin, policy definition and control
  ➢ Categorize by roles, groups, profiles for efficiency, accuracy
  ➢ Policy admin: manage resource access according to business and security policies
  ➢ Flexible delegated admin enables assigning a subset of admin authority to a designated user or group
  ➢ Self-service admin gives the user limited capabilities to add, modify, or delete information, password reset, subscriptions
  ➢ Accept identity assertions from third parties

• Expect integration with directory, access management
Architecture

Access management systems

• Combine scalable authentication, authorization
  ➢ Integrate with identity repositories: directory, database
  ➢ Integrate with identity management for delegated admin
  ➢ Integrate with multiple authentication systems (ID/password, NT, Windows 2000/AD/Kerberos, RADIUS, others…)
  ➢ Session management once a user is authenticated
  ➢ Integrate closely with applications/application servers
  ➢ Fine-grained rules: Identify a Web object by URL, operate at page, button or field level
  ➢ Flexible policy enforcement: Static, dynamic, ability to deal with variables: location, time of day, other attribute values
  ➢ Support for different models: groups, RBAC, rules
Architecture

Portals (presentation/personalization)

• Web-based systems aggregate content, services and applications into a single view or site, streamline delivery
  ➢ Ambiguous term; for our purposes, portals apply personalization, ACLs based on identity, preferences, roles
  ➢ Other functions, such as search, are outside I&AM scope
  ➢ Ideally, portals should leverage underlying directory, provisioning, and Web access management products
  ➢ Some integrate with access management systems, but few integrate well with directories
  ➢ Breadth, depth of connectors is primary value metric, but many connectors are simple pipes or “eye candy”
  ➢ As Web services gain adoption, connectivity will be overshadowed by identity, security, personalization
Architecture

Identity and access management infrastructure

- Admin, delegated admin, self-service
- Authoritative Directory
  - Users, groups, services
- Provisioning Services
  - Propagate Accounts & Privileges
  - Allow/Deny Access

- Identity Management
- Access Management System
  - Login
  - Authentication
  - Authorization
  - Presentation
- Portal

- Resources
  - Platforms
  - Applications
  - Databases
  - Resource Managers
  - Other Resources

Driving Network Evolution
Architecture

Market maturation (or lack thereof)

• Most of these technologies come from different vendors
  ➢ Overlap between products and approaches
  ➢ Burden of full integration is on the customer

• Consolidation across these functional categories has already begun, and the market will drive further consolidation over the next year to 18 months
  ➢ Early leaders battle for partners, market share
  ➢ Vendors strive for broad e-security positioning
  ➢ Big firms first partner with, then acquire smaller firms
  ➢ Vendors expand into ID management, portal, provisioning
  ➢ Combined solutions: PKI & access management, access management & directory, access management & portal
Identity and Access Management

Agenda

- Business drivers
- Architecture
- *Interoperability and portability*
Interoperability and Portability

Multiple drivers, a dichotomy of needs

• Internal enterprise issues have not abated
  ➢ Too many directories, fragmented identity infrastructure
  ➢ Error prone, expensive to manage
  ➢ How can enterprises integrate and leverage what they have?

• External B2B issues continue to build
  ➢ Do we have to synchronize every directory on the planet?
  ➢ Or can we make identity and entitlements portable?
  ➢ How will you authenticate users?
  ➢ Do hierarchical trust models work?
  ➢ What standards will emerge? And what about privacy?

• External public identity infrastructure wars heating up
  ➢ Passport, Liberty Alliance, Magic Carpet, etc.
Interoperability and Portability

The result: XML standards surge

- Security Assertions Markup Language (SAML)
  - Allows exchange of identity, authentication, authorization assertions between loosely coupled security domains
- XML Access Control Markup Language (XACML)
  - Richer XML constructs for authorization, access control info
- XML Key Management Services (XKMS)
  - Hope on the horizon for PKI-enabling applications
- Directory Services Markup Language 2.0 (DSML)
  - LDAP in XML clothing
- Service Provisioning Markup Language (SPML)
Interoperability and Portability

Realistic potential

• Why now and why XML?
• Alignment of market need, technology evolution
  ➢ The Web services framework promises a loosely coupled environment for application interoperability
  ➢ Simple Object Access Protocol (SOAP) provides XML protocol for a standard communication bus
• When coupled with that framework, these standards have significant potential to address the need for interoperability and federation for B2B applications
  ➢ Integrated internal environments capable of asserting information, communicating using SOAP and these XML standards
Interoperability and Portability

Public identity infrastructure

• Passport has a big lead, but Microsoft’s security problems create an opportunity for others
• You can’t eat just one
• Passport, Liberty Alliance, Magic Carpet, and others will force enterprises to address intersection between enterprise identity/role and public identity
  ➢ If your employees have a Passport or Liberty ID, can they use it internally?
  ➢ If they need a Passport or Liberty ID to access external services to do their jobs, how will you manage those IDs?
  ➢ If a partner’s employees have Passport or Liberty IDs, will you accept them? How will both you and the partner manage those IDs?
Interoperability and Portability

Public identity infrastructure

• Federation and interoperability are requirements
  ➢ Microsoft has proposed Kerberos, and since Catalyst Conference 2001 has softened its tone in regard to SAML
  ➢ Liberty Alliance has released precious few details, but it’s fair to assume that Sun’s investment in directory will play a significant role in what Liberty does
  ➢ AOL has quietly rolled out Magic Carpet, but no word on how federation will work
  ➢ Many of the same standards that are shaping B2B environments should/could apply to public identity systems
  ➢ In short, we are only at the beginning of the discussion, but the market will force federation to occur
  ➢ But don’t be surprised when it gets ugly
Interoperability and Portability

Integrated directory services enable federation

- Federated Directory Services (internal)
- Intranet
- Extranet/Internet
- Federated I&AM Services (SAML)
- PKI
- Meta-Directory
- Custom App
- E-mail
- Web
- E-biz Directory
- I&AM Services
- Enterprise Directory
- Migration to general purpose infrastructure
- Intranet
- Extranet/Internet
- Public Identity Services (Liberty, Passport, UDDI, Others)

The Burton Group
Driving Network Evolution
Interoperability and Portability

A final word on SSO

• SSO is a dirty word; expunge it from your vocabulary
  ➢ *Reducing* sign ons is a valid goal, but a *single* sign on is a security compromise waiting to happen
  ➢ Even if we achieve a standard authentication infrastructure that applications share, SSO is not realistic
  ➢ Different applications require different security, and different app states may require different security in a single app
  ➢ Policy should guide how and when challenges occur
  ➢ And one single credential of any kind should never give anyone access to everything

• Create integrated security architecture that relies on general-purpose mechanisms for integration and interoperability, but enables real security
Identity and Access Management

Conclusions

• The road to identity and access management infrastructure has curves, detours and construction zones
• The end destination and scenery along the way is well worth the journey—solid business justification is there for most large organizations
• Invest in general-purpose systems today
• Plan carefully, but be flexible
• Use the infrastructure to gain a strategic competitive advantage