



Network Identity: Unlocking the Value of Web Services

Phil Schacter
VP and Director
Directory and Security
Strategies
Burton Group

Tuesday, May 11 2:15 – 3:30

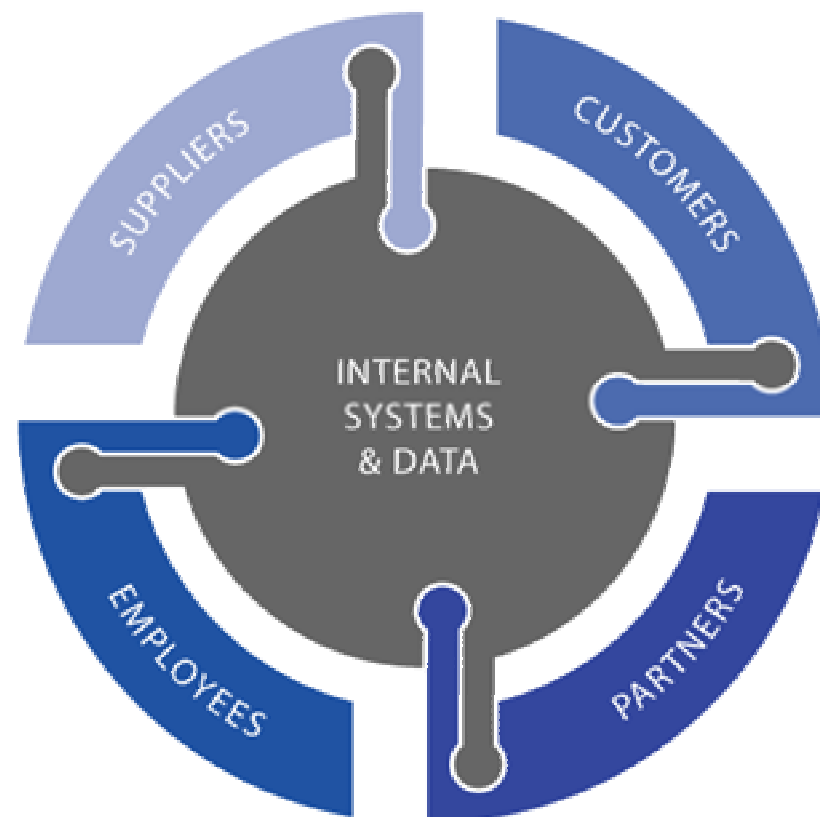
Identity and the Network Platform

2



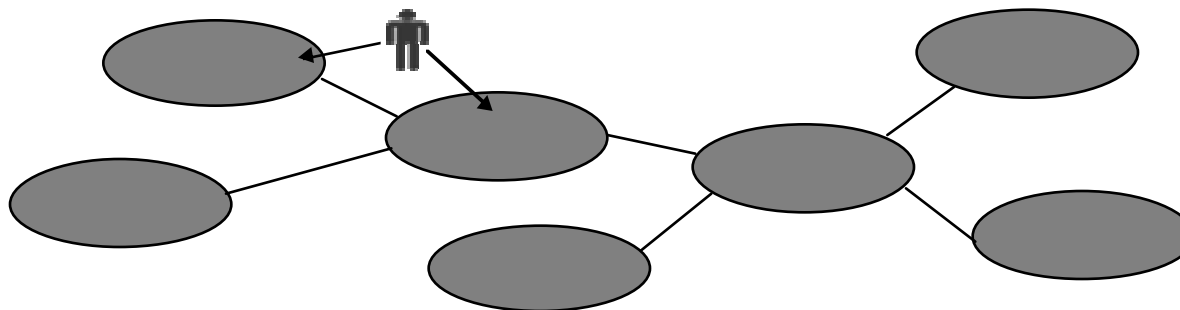
The virtual enterprise network

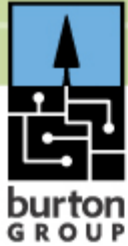
- Identity has become a strategic business issue
- Most of the activity around Identity Management (IdM) is occurring in the enterprise, as identity follows business to the digital domain
- Enterprises must both *open and protect* mission-critical systems, making them accessible independently of user location
- Web services and identity management are core infrastructure elements necessary to *enable* and *secure* the VEN



Identity Management Concepts

- What is Identity Management?
 - A set of processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities within a security domain
- What is Federated Identity Management?
 - Agreements, standards, technologies that make identity and entitlements portable across autonomous domains



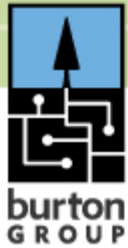


Identity and the Network Platform

4

Securing the Virtual Enterprise Network

- Perimeter security models necessary but insufficient
 - “Exclusionary” security models don’t enable business
- Identity enables “inclusionary” approaches, becoming portable across processes, spanning apps, organizations
 - Identity provides predicates for security, regulatory compliance, risk and liability management, other business functions
 - Today identity management is fragmented, standards evolving
 - But market pressures are driving significant progress
- Identity management (IdM) is a strategic business issue, and enterprises should make infrastructure investments



Web Services and the Network Platform

5

Enabling the virtual enterprise requires a “network platform”

- Much of the Internet’s potential untapped because the infrastructure doesn’t support necessary functionality
 - The focus is moving to end-to-end business process
 - OSes, app servers, languages will remain important components
 - But we need a set of common protocols, interfaces for communicating, sharing data, conducting transactions across all platforms
 - Enables the necessary network-wide integration and interoperability
 - Turns the network into the computer, creating a network platform
- Web services framework has taken steps in this direction
 - In spite of the hype, more progress than any other previous attempt
 - Web services or not, we have to solve this problem

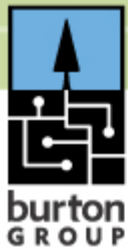


Identity Management and Web Services

6

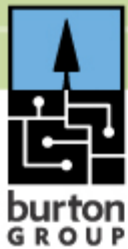
New approaches to integration and interoperability

- Next up, integration products and middleware: accommodating what you have
 - Large-scale, heavy-weight integration approaches are expensive, politically difficult, technically challenging
 - And such approaches simply won't work between domains
 - It was the only choice for a long time, but times are changing
- Tightly coupled integration approaches may still be necessary *within* security domains
 - But security must now span both logical, physical boundaries
 - And Web services cannot work without identity
- Federation and Web services standards will enable loosely coupled interoperability *between* security domains



Putting identity to work

- Federation will extend the reach, range of IdM
 - Internal federation can enable interop, consolidation after M&A
 - B2B connections can rely on identity-based security mechanisms
- Web services framework support for IdM standards will increase the ease of app development and integration
 - Core identity and security functions won't be orthogonal or bolted on
 - Consistent programming model, consistent tools, developer impedance matching, appropriate distribution of development burden
 - Security functions will become Web services, callable by average developers



Getting There: Trends and Directions

What infrastructure is needed for federated identity?

Public identity services, or other communities

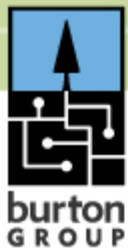
Identity Networks		
Ping Id	Verified	Shibboleth
.NET Passport	By Visa	Others

Used between or within Products / Domains / Services / Communities

Federated Identity Standards		
SAML	Liberty	WS-Security
WS-*	XACML	Others

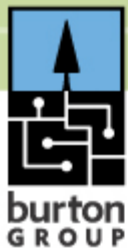
(Mostly) Used Within Domains

Base Security Capabilities		
Kerberos	LDAP	ID /Pwd
X.509	Token	RADIUS



Operationally, what's likely to happen?

- Federation begins at home
 - Will occur where business affinities already exist: between business units, between business partners
 - But this is not "plug-and-play"; it's "pay-to-play"
- Don't wait on the government to solve this problem
 - Governments will ultimately issue digital identities, pass laws, regulations that govern use, liability
 - But much of the law will trail market developments, conflicts
 - Won't establish business model; federation is up to relying parties
- Multi-party federations much more difficult to set up and administer than peer domain federation
 - Raises the question of identity "networks" and services



Federated identity standards and specifications

- Security Assertion Markup Language (SAML) has been standardized by OASIS
 - Provides authentication, authorization, and attribute assertions between loosely coupled domains
- Liberty Alliance has built on SAML to develop additional specifications
 - Opt-in account linking
 - Permission based attribute sharing
- WS-Security is being standardized by OASIS
 - Protects Web services messages
- WS-*: Microsoft, IBM and other vendors working on more Web services security specifications, such as WS-Federation

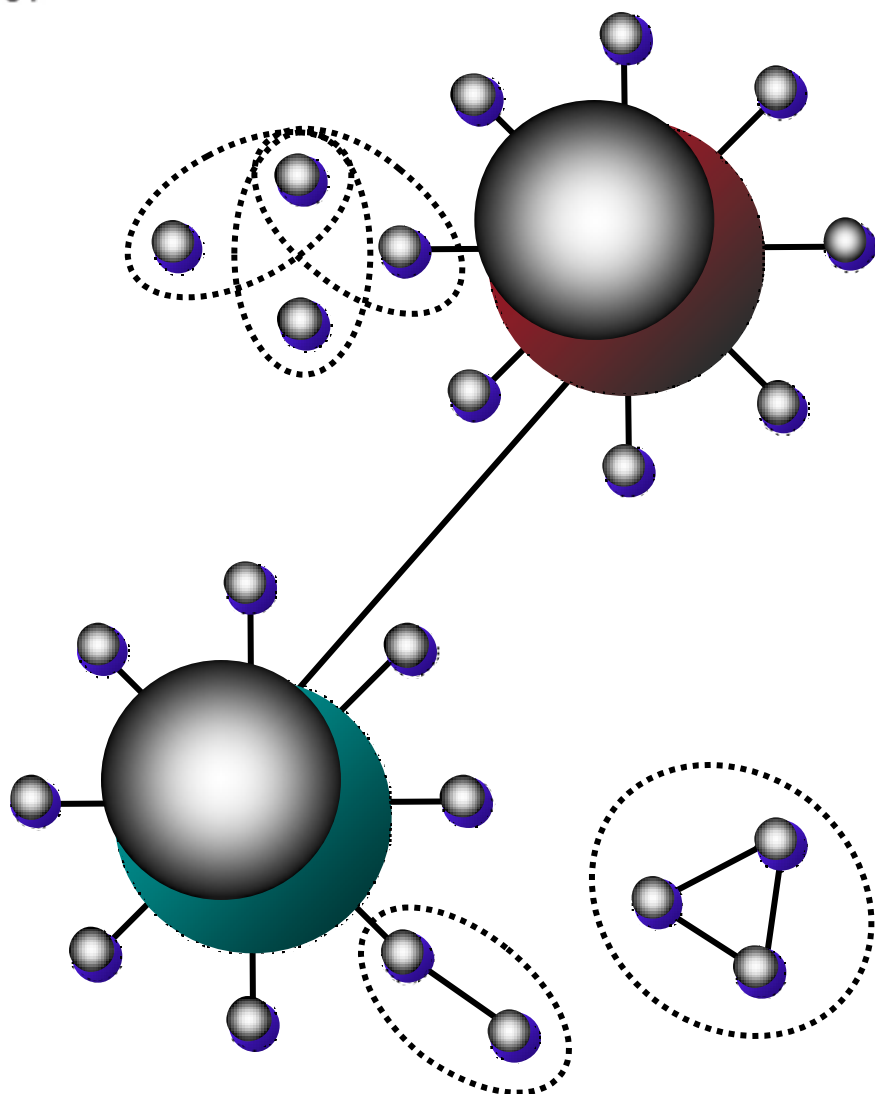


Identity networks: There won't be just one

- Centralized
 - Passport and AOL Screen Name Service
 - Passport has lots of IDs, but isn't really driving public identity
 - Security flaws, centralized architecture are continuing problems
 - Microsoft will re-invent Passport using federation, Web services
- Industry-based, proprietary:
 - SecuritiesHub/BondHub, Verified by Visa, others
- SAML-powered: Shibboleth, multiple corporate networks
- Liberty-powered
 - Corporate B2E and mobile projects underway
 - Neustar (eRX Land Records Exchange Network)
 - Financial networks (SecuritiesHub, others)



Federation implies a poly-centric environment



- Many islands will emerge
- Industry-specific solutions are likely
- How will they converge?
- Identity networks could emerge to link the islands
- Identity networks must federate, may be member-owned (as in the ATM, credit-card worlds), provide common governance and policy frameworks, or other models

..... Identity peering ● Identity domains



Waves of federated identity adoption

Increasing market size, complexity and value

First Wave

- Pair-wise relations
- SAML 1.1 and Liberty ID-FF
- SAML add-ons and SAML packages

2003 - 2004

Second Wave

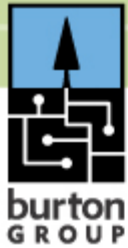
- Communities, Circles of trust
- SAML 2.0 (Liberty + SAML), WS-*
- Advanced federation products, services

2005 - 2007

Third Wave

- Dynamic Communities
- Built-in federation
- Identity networks

2008 - 2010



Identity and the Network Platform

14

Conclusion: A long, but inevitable transition

- Web services and federated IdM have enormous potential
 - Technology, legal, and business infrastructure must combine
 - Today, we're several years and many breakthroughs away
 - But the era of enterprise IdM and Web services has arrived
- Understand the link between Web services and IdM, and start defining architectures for supporting them
 - Some will be driven by carrots, others by sticks, most by both
 - All face a choice: Do it the old way, or build general-purpose architecture
- Enterprise digital IdM, federation will influence the future
 - Technologies, standards, law and policy governing enterprise IdM and public/individual digital identity will influence each other