Identity & Access Control in the Cloud

Lanling Wen
National Standard Officer
Microsoft Corporation

Nevin Dong
Platform Strategy Advisor (PSA)
Microsoft Corporation
Microsoft and OASIS

- Microsoft is one of the 4 top-tier “Foundational Sponsors” at OASIS
- Microsoft has chaired many OASIS technical committees and has a long history of board participation
- Microsoft has very publicly committed to “cloud technologies”
- We’re pleased to bring you this short report on Identity in the Cloud
Industry Trends Driving Customers & Vendors

**Externalization of IT**
Apps are on-premises, outsourced, in the cloud

**Consumerization of IT**
Users need access from anywhere & any device

**Virtualization of IT**
Collaboration creates virtual organizations

**Regulation of IT**
Regulatory compliance and Auditory oversight

**Regulation of Identity**
Government provider & consumer of digital IDs

**Explosion of Information**
Globally dispersed data needs to be protected
Trends create Challenging Demands on IT

Existing IT Practices

- Corporate **assets are inside the perimeter**. Users **enter the perimeter** to access the assets.
- IT has physical or contractual (outsourcing) **control over corporate data**.
- Employees centrally identified; everyone else must be kept out.
- Authorization can be **managed centrally** by IT per individual asset.
- Supply chains are static enough to be **managed via internal user accounts**.
- Devices are **managed PCs**, domain-joined and fully trusted by IT.
- Compliance controls based on **perimeter** and **centrally managed** access policies.
- IT is a **Cost Center**. Large staffs for custom application development and entitlement.

New World Order

- Corporate **assets are everywhere**. Users need to **access assets from anywhere**.
- Virtual orgs & cloud require **data protection** outside IT control scope.
- Mergers and collaborations dynamically change **trust relationships and user populations**.
- Authorization **manageable** by Business Owners but in compliance with corporate policy.
- Partner, customer & retiree **identities originate anywhere**.
- **Continuum of devices** managed & unmanaged, organizationally & privately owned.
- Ensure **compliance everywhere** on top of 3rd party infrastructures with restricted visibility.
- IT must **increase corporate agility** in getting new value to the marketplace.
Identity in the Cloud ... the Possibilities

Trustworthy data sources:
- Identity Providers
- Attribute Authorities

Secure mechanisms:
- Strong authentication
- Protect data on corporate and personal devices

Governance:
- Trust framework
- Accreditation & audit
- Incident reporting

Cloud Identity Services:
- Works on behalf of Users and Relying Parties
- User profiles with Privacy enhancing technologies
- Claims normalization and interoperability
- Coordinated access control “safety net” across RP sites

Relying Party:
- Policies on required user data & how it can be used
- Policies on organizational data protection
- Audit trails
- What-if and historical authorization analysis
Microsoft Cloud

PUBLIC

Windows Azure

PRIVATE

Windows Server with Hyper-V

Traditional Datacenter

Highly Virtualized Datacenter
Authenticating Users from Web and Social Providers

Sign-up and claims enrichment

Windows Azure
Identity in the Cloud ... the Vision

Bring **User-centric Identity** (self-control & privacy) and **Business-centric** (bottom line & compliance) **Identity Management** together by empowering users to seamlessly access the right resources from anywhere and any device, while enabling business administrators to easily control and protect those resources.
Thank you!

Merci  谢谢您  Grazie  Danke  谢谢您

Bedankt  Obrigado  Gracias  Takk