Recommendations for Institution Wide Smart Card Best Practice

Paul Conroy

Technology Specialist
Identity and Access Management
Microsoft

paul.p.conroy@microsoft.com

Agenda

Business Drivers

Methods to achieve success

- -Governance
- -Staged approach
- -Technical framework
- -Workflow enablement
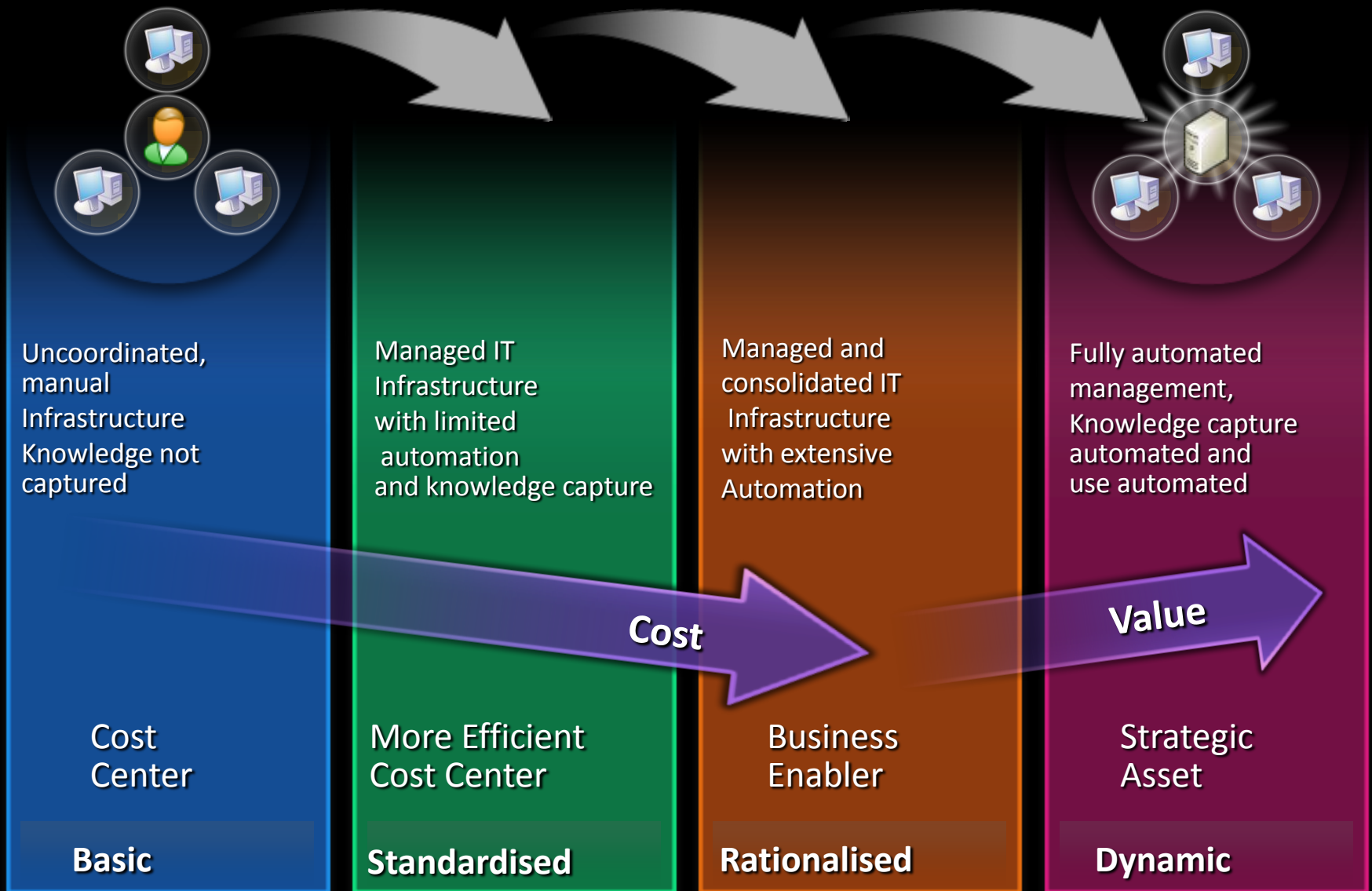
Next steps

Q & A

Business Drivers

- Productivity
  - session preservation

- Cost reduction
  - Pin reset cost US$30

- Security
  - 2 Factor to protect "keys to the kingdom"

Source- Optimising Infrastructure: The Relationship Between IT Labour Costs and Best Practices for Identity and Access Management with Active Directory

Methods to Achieve Success

- Governance

- Staged Approach

- Technology Framework

- Workflow

Governance

Uncoordinated, manual Infrastructure Knowledge not captured	Managed IT Infrastructure with limited automation and knowledge capture	Managed and consolidated IT Infrastructure with extensive Automation	Fully automated management, Knowledge capture automated and use automated
Cost →		**Value** →	
Cost Center	More Efficient Cost Center	Business Enabler	Strategic Asset
Basic	**Standardised**	**Rationalised**	**Dynamic**

IDA Optimisation Model

Basic	Standardised	Rationalised	Dynamic
Directory Multiple Login Points To Resources	A Primary Directory Used to Authenticate Users To Windows Applications	A Primary Directory Used to Authenticate Users to Non-Windows Apps	Employee Authentication Extended Outside The Enterprise
Lifecycle No Formal Lifecycle Processes	Directory Data & Workflow Process Standardisation	Metadirectory Used to Keep Information Synchronised	Identity Lifecycles Managed Via Policies & Workflow
Info Protection Physical Protection	Encryption-Protected Content	Enterprise Rights Management (ERM) & Mobile devices	Policy-Based ERM Across Partners & Customers
Strong Authentication User IDs and Password	Strong Password Policy enforcement	Multi-Factor Authentication Used For High-Risk Scenarios	Multi-Factor Authentication Used For All Corporate Applications & Users
Federated Identity Multiple User IDs	One User ID & Password For All Extranet Applications	Federated Trust Used Instead of Extranet User ID & Password	Federated Trust Applied To Web Services
Cost Center	**More Efficient Cost Center**	**Business Enabler**	**Strategic Asset**

Basic	Standardised	Rationalised	Dynamic
Lifecycle No Formal Lifecycle Processes	Directory Data & Workflow Process Standardisation	Metadirectory Used to Keep Information Synchronised	Identity Lifecycles Managed Via Policies & Workflow
Strong Authentication User IDs and Password	Strong Password Policy enforcement	Multi-Factor Authentication Used For High-Risk Scenarios	Multi-Factor Authentication Used For All Corporate Applications & Users
Cost Center	**More Efficient Cost Center**	**Business Enabler**	**Strategic Asset**

Staged approach

…and the alternative
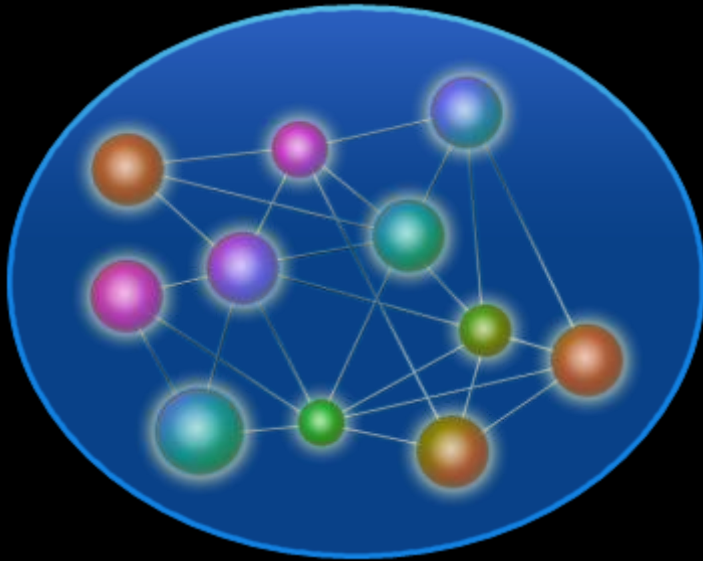
Option 1: All at once

- Target connecting everything at once
- Complete infrastructure and data synchronisation and process rationalisation

Option 2: Step-wise approach

- Start with the directory and metadirectory basics
- Create a basic lifecycle solution and then build incrementally on it
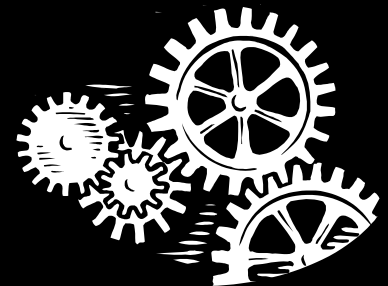- Prioritise strong authentication, federation, and information protection
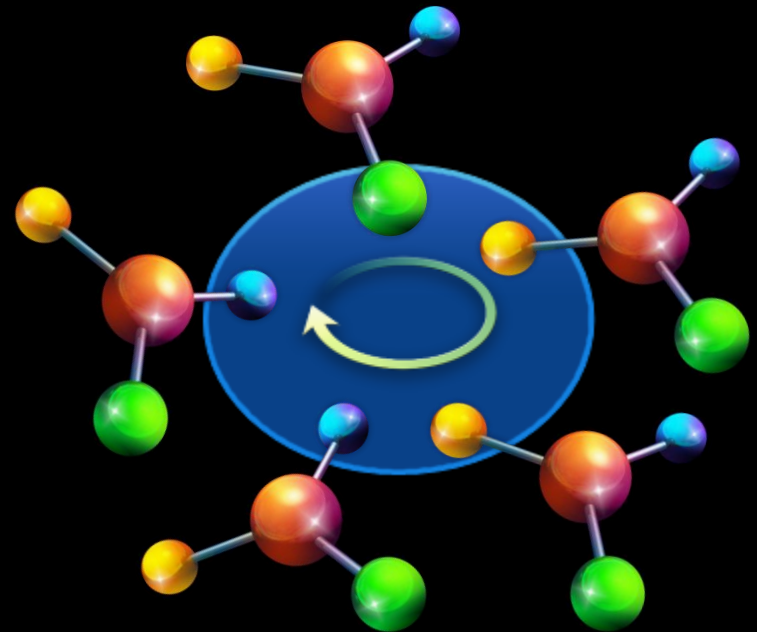
Technology Framework

- Digital Certificates

- Physical access – Radio Freq. ID – Photo ID

- Synchronisation of relevant systems

Workflow

- Enrollment
- Replacement
  - Temp Cards
- Revocation
- PIN Mgt
  - Unblocking

Next steps….

Information from the Microsoft Identity and Access (IDA) Microsite

Visit http://www.microsoft.com/ida

WHITE PAPER

Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Identity and Access Management with Active Directory

Sponsored by: Microsoft

PCs managed by Group Policy Objects (GPOs)

Comprehensive directory solution

Reduction of third-party application directories

Automated user provisioning

Q & A