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”

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 Center

More Efficient Cost Center

Business Enabler

Strategic Asset

Basic

Standardised

Rationalised

Dynamic
### IDA Optimisation Model

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

- **Info Protection**
  - Physical Protection

- **Strong Authentication**
  - User IDs and Password

- **Federated Identity**
  - Multiple User IDs

- **Lifecycle**
  - No Formal Lifecycle Processes

- **Directory**
  - Multiple Login Points To Resources

- **Business Enabler**
  - More Efficient Cost Center

- **Strategic Asset**
  - Business Enabler

- **Dynamic**
  - Federated Trust Applied To Web Services

- **Enterprise Rights Management (ERM)**
  - Managed Via Policies & Workflow

- **Federated Trust**
  - Used Instead of Extranet User ID & Password
**Strong Password Policy enforcement**

**Multi-Factor Authentication Used For High-Risk Scenarios**

**Multi-Factor Authentication Used For All Corporate Applications & Users**

**Lifecycle**
No Formal Lifecycle Processes

**Strong Authentication**
User IDs and Password

**Directory Data & Workflow Process Standardisation**

**Metadirectory Used to Keep Information Synchronised**

**Identity Lifecycles Managed Via Policies & Workflow**

**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