Identity Management

April 12, 2007

ISACA®

Your Speakers

Daniel R. Sterba, CISA

Program Manager

Enterprise Financial Services – SOX

Sprint Nextel Corporation

Alfie A. Mahmoud, PE, CISA, CIA

Senior Manager

IT Advisory

KPMG LLP

Objectives - Attendees

- What does Identity Management (IDM) mean to you or your organization?
- What are your objectives for the presentation today?

Objectives

1. At the end of this presentation, you should have a better understanding of:
   - What Identity Management (IDM) is and does
   - IDM's evolution
   - Common IDM business drivers
   - Common components required to facilitate successful IDM deployment (and risks to successful implementation)
2. Share IDM experiences in practice
3. Address attendee objectives and answer questions

Section I

Identity Management – what it is, what it does, evolution and business drivers

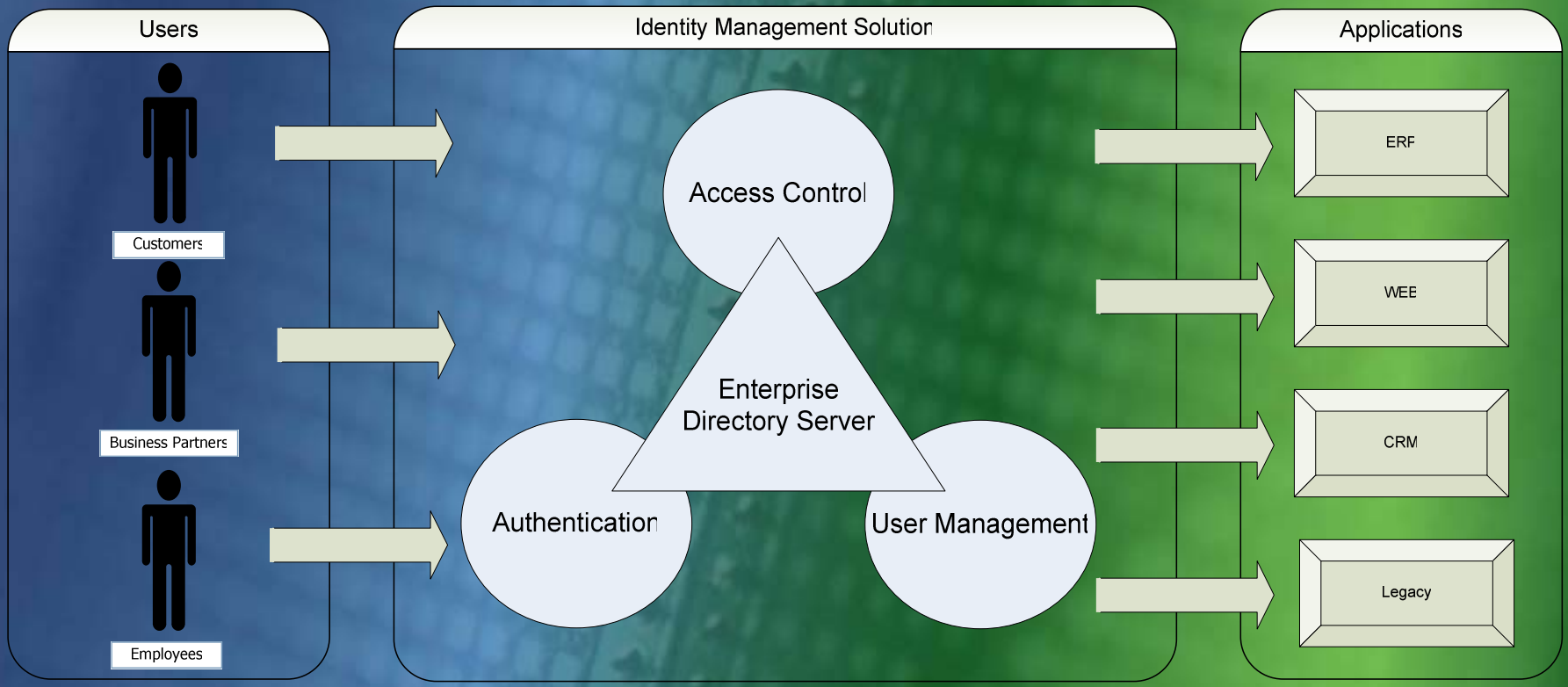
IDM - What it is and what it does

- Identity Management (IDM)
  - The process of managing the information for a user's interaction with an organization
    - Employees (including contractors)
    - Customers and Business Partners
- Ensures that the right people, including customers, business partners and employees have the right access to the right resources.

IDM's Four Components

1. Enterprise user directory
   - Directory services database
   - Meta-directory data integration service
2. Authentication
3. Access control
4. User management

IDM's Four Components (continued)



IDM – An Evolution

- Access administration typically performed manually system-by-system
- Inefficient and costly driven by
  - Increase in number and complexity of systems
  - Increase in number and type of users
    - Internal users
    - Customers and business partners

IDM – An Evolution (continued)

- Cost and complexity may impede development and deployment of new systems
- Drives the need and subsequent development of tools and methodologies to improve access administration
  - National Institute of Standards and Technology (NIST) Role Based Access Control (RBAC)
  - Extensible Markup Language (XML) based security specifications
  - Methodologies from Universities such as MIT and Stanford
  - Vendor and service provider tools and methodologies

Common IDM Drivers

- Improve user administration efficiency/reduce costs
  - Streamline provisioning and de-provisioning
    - Account setup and modification
    - Resource assignments
    - Role and rule assignments
  - Reduce cost of user administration
- Consistently enforce security policy
  - As the number of systems and users increase, so does risk
    - Drives investment in security controls

Common IDM Drivers (continued)

- Improve compliance
  - Privacy
  - Regulatory
- Increase usability
  - Increase user productivity and satisfaction
- Business strategy enablement
  - Shift to the Internet as a primary medium for conducting business
  - IDM may reflect upon how well an organization manages its business relationships
  - Reduce time to market for new initiatives

Section II

Common components required to facilitate successful IDM deployment (and risks to successful implementation)

Define the End State

- Needs to be clearly defined!!!
  - What will be included???
    - Alignment of identity information
    - Workflow task automation
    - Roles and rules-based authorization
    - System-wide auditing and reporting
    - Password self-administration
- Align with enterprise capabilities & objectives

Executive Support

- Why should IDM be implemented?
- Executive endorsement
- Set expectations
  - Link expectations to end state

Stakeholder Commitment

- Senior management
- IT management
  - User administration
- End users

Roles vs. Rules - Background

- Must be clearly defined
  - Basis for user administration and access control
- Background
  - Roles
  - Rules
  - Role-based access control (RBAC)
  - Rule-based access control

Integrating Roles and Rules

- Involvement of IT (e.g., user administration) and business management
- Find a balance
  - Risk/Reward
  - Ease of administration
- Use of rules to complement roles

Defining Budget

- What are we trying to accomplish?
  - Link to end state
    - On-boarding/off-boarding users
    - Password management
    - Role/rule based security
    - In-scope processes
- Vendor vs. in-house development
- How will the cost be split between IT and business?

Define Timeline

- Define timeline
- Milestones
- Project completion date
- Time constraints

Packaged or Custom Solution

- Package Solutions
  - Business practices may need to change to work with a packaged IDM solution
    - Minimal customization requiring business to fit the package)
- Custom Solution
  - A custom tailored solution can be created around current business practices
    - Minimal change to business practices

Packaged or Custom Solution (continued)

- Growth
  - Is scalability or flexibility important
    - Custom solution may not be able to grow with the company
- Competitive Advantage
  - Standards-based, stable systems
  - IDM as a differentiator

Packaged or Custom Solution (continued)

- IT budget
  - Minimal IT budget needed with vendor implementation
  - Custom development will require an extensive IT budget
- Time
  - In house custom development typically takes longer to implement

Project Management Structure

- Keep end-state in mind
- Monitor budget and timeline constraints
  - Milestone tracking
- Vendor vs. in-house Project Management (PM) role
  - Expertise
- PM as liaison between IT and business

Phased Implementation

- Developing an overall implementation plan and testing it on a small scale using production data
- Making sure that all participants understand the objectives and know where to go for help
- Starting with good data and being prepared to refine the data
- Establishing reasonable, tractable measures of success
- Preparing to deal with the unexpected
- Institutionalizing the process once in place

Additional Requirements to Define

- Defining requirements is complex in any environment
  - Define methodology
    - Roles and rules (discussed earlier)
  - Data integrity - plan for the worst, hope for the best
  - Legacy systems
  - Existing user administration processes and tools
    - Useful or sunk costs?

Attributes of Successful Implementations

- Monitoring progress
  - Budgets
  - Unreasonable timelines
- Project size and complexity
  - Scope creep monitored and controlled
- Discover and manage gaps
- Choose the right staff
  - Monitor staffing and turnover
  - Project scheduling
  - Prevent knowledge leak

Section III

IDM Examples in Practice – Considerations and Benefits

Effective Planning

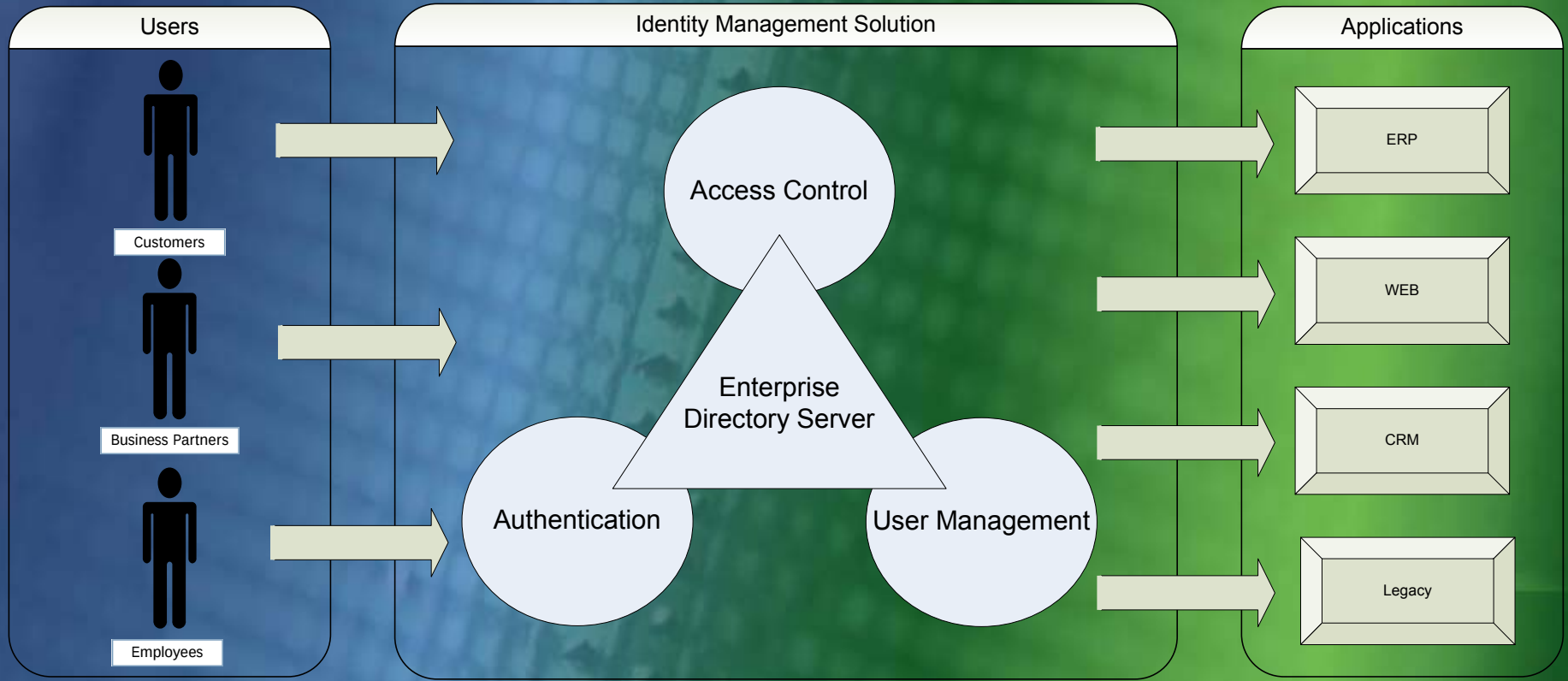
- Allocate appropriate time/resources for effective planning to occur
  - Engagement across the organization
  - Cost savings in the long run
- Perform Planning for each of the four IDM components
  - Consider ‘source of truth’ for employees and non-employees
  - IDM interfaces and associated controls

Testing Importance

- Allocate appropriate time/resources for thorough testing
- Test parallel to Production over a period of time

Phased Approach

- Enterprise User Directory as foundation
- What degree of IDM should a company have?
- Automation



Benefits in Production

- Data Integrity
  - One source data repository
  - Common Processes
  - Elimination of one-off workflow tools
- Automation
  - On-boarding and/or provisioning
  - Terminations (Off-boarding)
  - Monitoring

Benefits in Production (continued)

- Centralized Security Function
  - UAM (User Access Management)
    - Data Integrity
    - Monitoring capabilities
    - Reduction in management testing and audit fees
  - Increase Productivity

Questions and Answers

Q&A

Contact Information

Daniel R. Sterba, CISA

Program Manager, Enterprise Financial Services – SOX

Sprint Nextel Corporation

Office: (913) 315-7472

Cell: (816) 686-7299

Email: Dan.R.Sterba@sprint.com

Alfie A. Mahmoud, PE, CISA, CIA

Senior Manager, IT Advisory

KPMG LLP

Office: (816) 802-5637

Cell: (913) 907-4029

Email: amahmoud@kpmg.com