

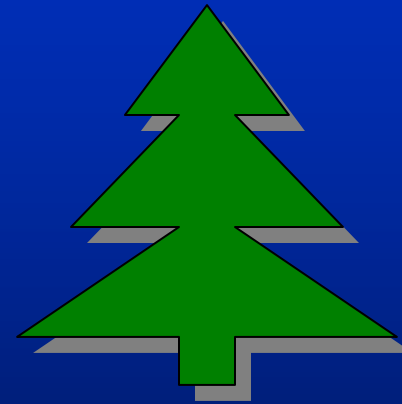
120 – Identity Management – The Password Jungle and the Quest for Single Sign-on

David Treece
Steve Wyatt

22 May 2006
1:10 pm

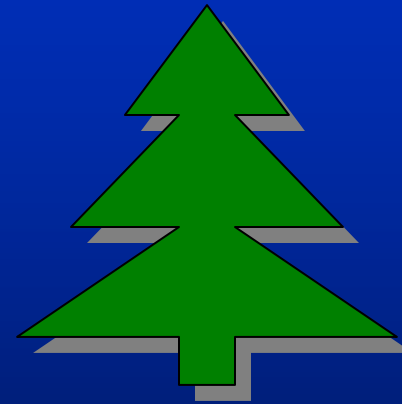
The Password Jungle?

- Boot up passwords
- Screen savers
- Network access
- Remote access
- Operating systems
- Authentication tokens
- Business applications
- . . . Plus personal . . .



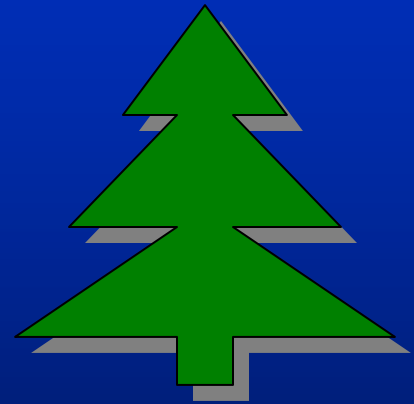
The Password Jungle?

- Problem with:
 - Quantity & Quality
 - Synchronization
 - Complexity & Aging
- Just a few “trees”.
- **Identity & Access Management (IdAM)** is the real Jungle!



Password Jungle?

- IT technical problem?
- Can it be solved with:
 - Scripts & coding?
 - Scripting with “bolt-ons”?
 - Retinal scans?
 - Biometric devices?
 - “Smart Cards or Appliances”



IdAM

- The set of processes, tools and policies that:
 - Verifies WHO a user is
 - Defines WHAT a user is authorized to access
 - Tracks WHAT a user actually accessed
 - Defines WHAT a user may do
 - Limits HOW or with WHOM information may be shared
- all while ensuring compliance to government and Corporate policy

IdAM - is not

- Single sign-on (SSO)
- A technology
- A band-aid
- Something that is done all at once
- An issue solved with a Purchase Order
- A checklist item that gets marked “Done”

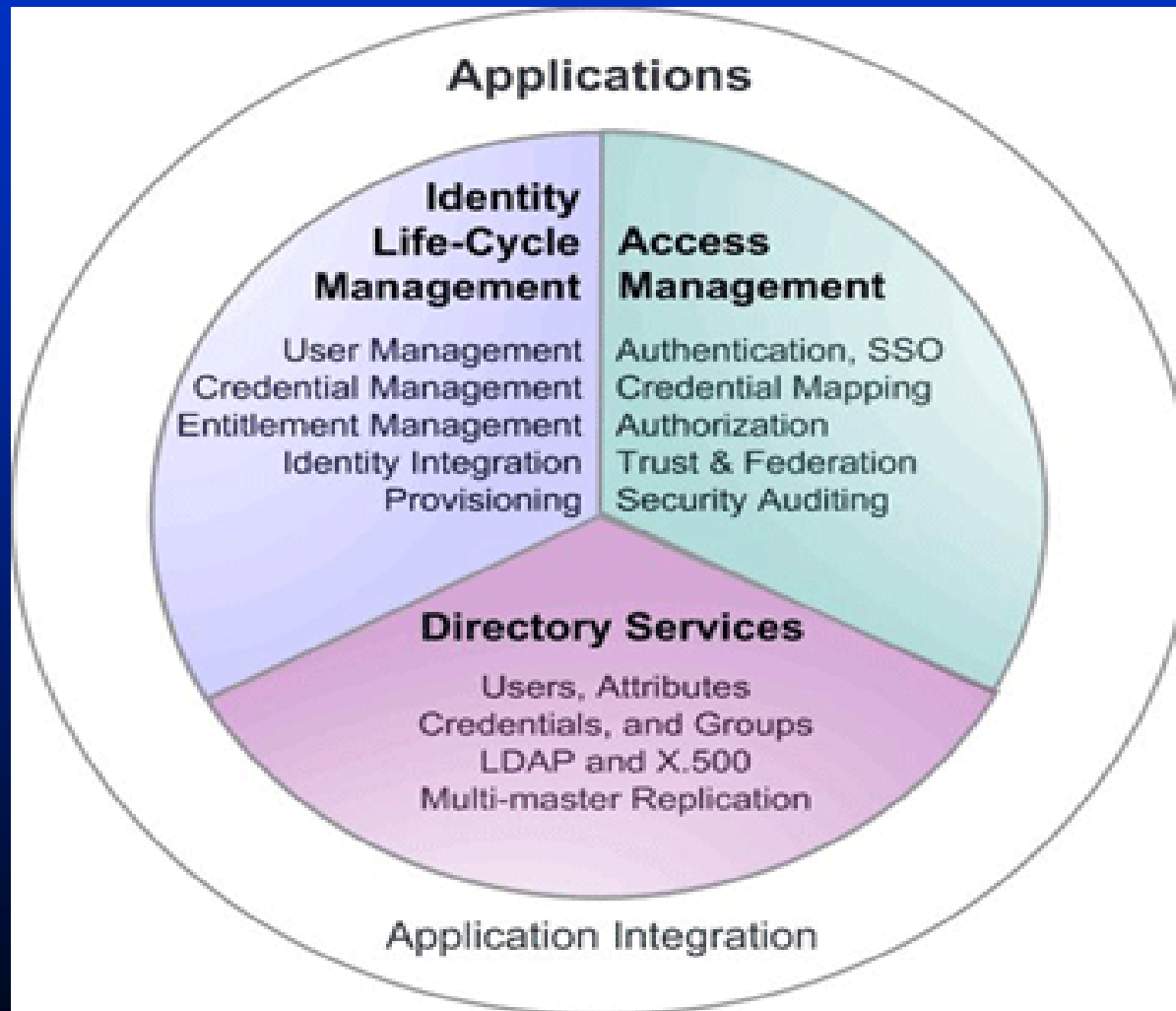
IdAM

- Establishes and manages the identity of a person throughout the entire life cycle of that identity
- Uses policies to define access rules to the resources the person requires to perform their job
- Defines what a person may do with the allowed resources
- Enforces access control across the extended enterprise

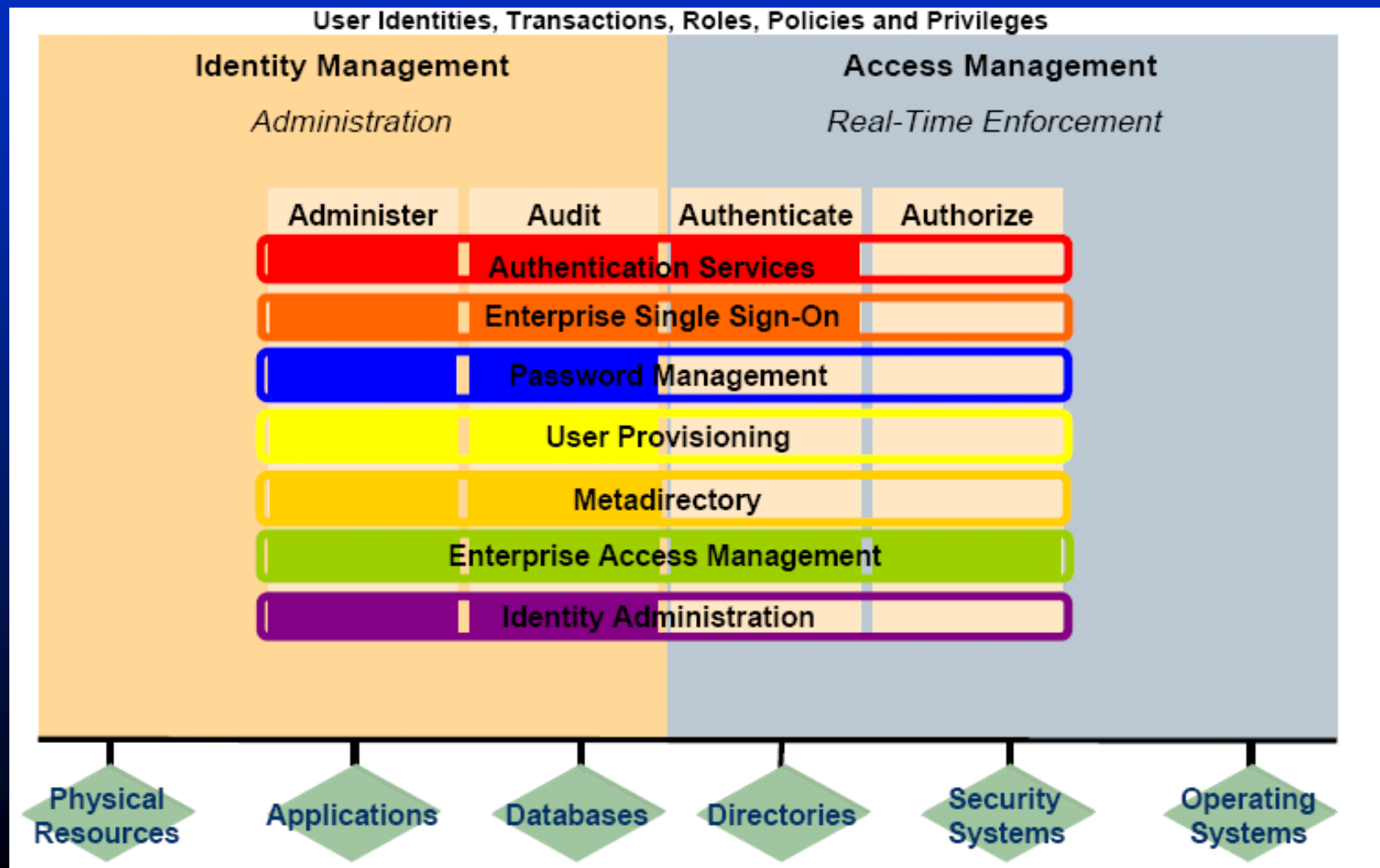
IdAM

- Facilitates processes for:
 - Access approval
 - User provisioning
 - Compliance reporting
- Manages information privacy in accordance to local law and Company requirements
- Consolidates and integrates identity functions, directories and data stores
- Ensures security compliance with Corporate policies

IdAM – per Microsoft



IdAM – per Gartner



IdAM

- Identity Management: (part A)
 - User Management
 - Credential Management
 - Entitlement Management
 - Identity Integration
 - Provisioning & De-provisioning



IdAM

- Access Management: (part B)
 - Authentication & Single Sign-on
 - Credential Mapping
 - Authorization
 - Trust & Federation
 - Security Auditing



IdAM

- Directory Services: (part C)
 - Users & Attributes
 - Credential & Groups
 - LDAP
 - x500
 - Multi-master Replication



Approach to IdAM

- What are the business drivers?
 - Specific requirements of Identity Management for near- and long-term business initiatives?
 - What privacy regulations or policies apply?
 - What are special trading partner considerations?
- What are economic drivers?
 - Reduce Operating, Help Desk, Admin costs
 - Top-line growth through new channels or services

Approach to IdAM

- Define Security Strategy
 - Scope of authenticated access (internal, external, biometric, encryption, etc)
 - Scope of integration
 - Limitations for self-service and separation or duties
 - Handshake points with service provider(s)
- Outline Business Case
 - ROI Analysis
 - Risk Assessment(s)

Approach to IdAM

- Develop Architectural Roadmap
 - Make a clear decision on either an application approach or an infrastructure approach
 - Application approach is generally a quick fix, low initial cost, “good enough”, stop gap, point solution.
 - Infrastructure approach is a broader solution, more expensive, tightly integrated, flexible, process oriented, strategic
 - While the technology is challenging, the real issues are organizational

Approach to IdAM

- If a clear decision to pursue IdAM, then
 - Engage Corporate Leadership for Policy Guidance
 - Engage HR and IT Security for policy definitions
 - Engage Application Development for data store development, refresh and integration
 - Engage Communications to spread the word
 - Engage the entire user community, internal and external, to appreciate and accept the heightened level of security

IdAM @ Sonoco

- Architecture framework:
 - Microsoft Identity Integration Server (MIIS)
 - Interfaces with:
 - PeopleSoft HRIS, Lotus Notes, SQL
 - Active Directory & AD/AM
 - ADAM (LDAP Directory)
 - “Information objects”:
 - User Profile, organization, relationships,
 - Applications, entitlements
 - Ultimus Workflow Engines & Forms
 - MS/SQL for MIIS/ADAM, Ultimus & Audit History

IdAM @ Sonoco



IS Service Requests

[Add New Account](#)

[Modify User Profile](#)

[Change PIN](#)

[Add User Services](#)

[Change User Services](#)

[Remove User Services](#)

[Transfer Account](#)

[Terminate Account](#)

[Request Status](#)

Hello **TAMMY LAWSON**. Your NT account is: **lawsonta**.
Your manager is: **DEBORAH MCCRACKEN**. Your location is: **Forest Products**.

Available Applications: (Note: apps you already have are not shown.)

- | | | |
|--|--|--|
| <input type="checkbox"/> ARX | <input type="checkbox"/> Hyperion | <input type="checkbox"/> PCard |
| <input type="checkbox"/> BaaN | <input checked="" type="checkbox"/> IBM | <input type="checkbox"/> PeopleSoft
Financials Access |
| <input type="checkbox"/> Consumer
SharePoint | <input type="checkbox"/> Industrial
SharePoint | <input type="checkbox"/> ProfitKey |
| <input type="checkbox"/> Corporate
SharePoint | <input type="checkbox"/> M2K | <input type="checkbox"/> Project Tracking |
| <input type="checkbox"/> DISPATCH | <input type="checkbox"/> Man Power
Internet Reports | <input type="checkbox"/> SBT |
| <input type="checkbox"/> eCore | <input type="checkbox"/> Omega | <input type="checkbox"/> SEDMS |
| <input type="checkbox"/> EDI | <input type="checkbox"/> Optivision | <input type="checkbox"/> TQMP |
| <input type="checkbox"/> Fixed Assets | <input type="checkbox"/> OTG for Financials
Access | <input type="checkbox"/> TSO |
| <input type="checkbox"/> Flexibles Baan | <input type="checkbox"/> Paper Costing | <input type="checkbox"/> UNIX |
| <input type="checkbox"/> Foldware | <input type="checkbox"/> Paper Reporting | <input type="checkbox"/> UNIX Access |

IdAM @ Sonoco



IS Service Requests

[Add New Account](#)

Hello TAMMY LAWSON. Your NT account is: lawson.ta.
Your manager is: DEBORAH MCCRACKEN. Your location is: Forest Products.

[Modify User Profile](#)

[Change PIN](#)

[Add User Services](#)

[Change User Services](#)

[Remove User Services](#)

[Transfer Account](#)

[Terminate Account](#)

Employee Name:	TAMMY LAWSON	Employee Type:	S
Employee Code 1:	F	Employee Code 2:	R
Employee Status:	A	E-mail Address:	tammy.lawson@sonoco.com
Business Unit:	US001	Plant:	A000
Department:	61001	Building:	Forest Products
Room:		Mail Stop:	M07
Telephone Number:	843/383-7936	Fax Number:	

Approving Manager: DEBORAH MCCRACKEN Division Administrator: [Unknown]

[Request Status](#)

Your current apps are shown below. Please select those you wish to remove.

- Ariba Lotus Notes Travel Card
 Content Management System Secure ID

Submit

