What is Secure Identity Management (SIM)?

Chris Van Den Abbeele
Cvdabbeele@novell.com
I. Where is the pain in IT Identity and Access Management?

II. What can Secure Identity Management (SIM) do for you?

III. What are the Building Blocks of Identity and Access Management?

IV. Identity and Access Management Solutions

V. Return on investment

VI. Listen to the Analysts

VII. Customer References
Novell one Net

Business Requirements

• A world without Information Boundaries means:
  • Access to IT Services and Information Assets
  • By anyone, from anywhere
  • In a Secure and Relevant way, based on Identity

Existing Systems

Network  Collaboration  Docs/Content  Utilities  Transactions  Packages
I. Where is the pain in IT Identity and Access Management?

- too many passwords
- too many user-ids
- no integrated view on security
- no central (cross platform) identity management
II. What can Identity and Access Management do for you?

First get rid of the confusion

- for a Network Administrator?
- for an Application/Platform/Database Administrator?
- for a Human Resources Manager?
- for a Network User?
- for the Security Officer?
- for a CxO?
II. What can Identity and Access Management do for you?
First get rid of the confusion

- for a Network Administrator?
  - Create an account once and only once
  - Update / maintain / lock an account once and only once

- for an Application/Platform/Database Administrator?
  - A threat?

- for a Human Resources Manager?
  - At least consistent user information across the enterprise

- for a Network User?
  - Login once and only once
  - Have access to all my resources (from any location, at any time, using any device)
II. What can Identity and Access Management do for you?

First get rid of the confusion

**for the Security Officer?**
- Setup a comprehensive and centralized security system
- See the “full picture” of a person again
- Man in the middle attacks?

**for a CxO?**
- Another step in becoming an “Agile Enterprise”
- Compliancy (ISO, FDA, …)
- Do more with less…
II. What can Identity and Access Management do for you?

*more confusion*

- What is “one password”?
- What is “Single Sign On”?
- What is “one identity”?
- Who owns the identities?
II. What can Identity and Access Management do for you?

*more confusion*

- What is “one password”?  
  - The same password for every application/platform?  
  - Enter my password only once (when I logon to the network)?
- What is “Single Sign On”?  
  - How would you set it up?
- What is “one identity”?  
  - Where is it stored?
- **Who owns the identities?**  
  - Authoritative data sources  
  - Delegated administration
II. What can Identity and Access Management do for you?

**conclusion**

- Secure Identity Management has a different meaning, depending on who you talk to, make sure everybody knows exactly what you talk about

- so... what are we talking about?
Secure Identity Management

Provisioning and Account Management

Access Management

Audit

Auditor or Administrator

NT/2000/XP
Host
Directory

Firewall/VPN

Employees

Customers

Partners / Suppliers

Web Servers

Web Access Management

Federated Identities

Other Organizations
Novell Nsure Secure Identity Management

- eDirectory
- DirXML
- Nsure Resources
- Novell Account Management

- eDirectory
- Host
- Directory

- NT/2000/XP
- Host

- SecuredLogin
- Sign-on (SSO)

- SecuredLogin
- Employees

- BorderManager

- SecureLogin
- Employees

- iChain
- Web Access Management
- SAML Liberty

- Web Access Management
- Web Access

- Web Servers

- Auditor or Administrator

- Customers
- Partners / Suppliers

- Web Servers

- Nsure Audit

- Customers
- Partners / Suppliers
II. What are the Building Blocks of Identity and Access Management?
III. What are the Building Blocks of Identity and Access Management?

*Build on the right “Platform”*

<table>
<thead>
<tr>
<th>Identity Driven Solutions</th>
<th>Secure Identity Management</th>
<th>Novell Nsure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Management</td>
<td>Access Management</td>
<td>Identity</td>
</tr>
<tr>
<td>User-Provisioning</td>
<td>Federated Authentication</td>
<td>Integrated Identity</td>
</tr>
<tr>
<td>Web Access Control &amp; SSO</td>
<td>Account Restrictions</td>
<td></td>
</tr>
<tr>
<td>Resource Mgt &amp; Web Services</td>
<td>Secure Logging &amp; Auditing</td>
<td></td>
</tr>
<tr>
<td>Application Integration &amp; Portals</td>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Etc.</td>
<td>Notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
III. What are the Building Blocks of Identity and Access Management?

*Build on the right “Platform”*

Layer I: Integrate your identities
III. What are the Building Blocks of Identity and Access Management?

*Build on the right “Platform”*

What is the most basic Identity Management Solution?

- the Identity Vault

  - Meta engine must do a secure-bind to data sources
  - Authoritative Data Sources
  - Common ID?
  - CEO sponsorship

Caveats:
- Data Ownership
- Clans
- Legacy Apps?
- Security?

Providing identity data from/to each application

- Authoritative Data Sources
- Common ID?
- CEO sponsorship
III. What are the Building Blocks of Identity and Access Management?

*Build on the right “Platform”*

Layer I: Integrate your identities

- the Identity Vault
  - multi-master, high available, cross-platform, multi-protocol, ...
- LDAP authentication alone is not the solution
- Data Ownership and Clans
- Meta engine must do a secure-bind to data sources
- Authoritative Data Sources
- Common ID?
- CEO sponsorship
Creating a complete identity from multiple authoritative sources

Enterprise Identity
Name: Julie Smith
DOB: 27 - July - 1963
Salary: level 22
E-mail: jsmith@acme.com
Phone: 408.555.1234
Prefs: 

A Single Virtual Identity... for employees, customers, partners, suppliers, etc.

Identity and Access Management Policies Implemented and Distributed Reliably as System Rules

Policy

Rule

Portions of Identity Managed by Appropriate Groups

HR
Finance
IS&T
Web
PBX

Self-service portal
Quick Win:
A Self Maintaining “Who is Who”

Data is replicated
• from Human Resources
• from PBX (Tel)
• from eMail
• ...

[Image of a self-maintaining directory system]
Quick Win: A Self-Maintaining “Who is Who”

Since Data is replicated in real time from the Human-Resources (HR) system, we can auto-generate an Org. Chart.
III. What are the Building Blocks of Identity and Access Management?

*Build on the right “Platform”*

Layer II: Manage your Identities

- Identity Driven Solutions
  - Password Management
  - User-Provisioning
  - Web Access Control & SSO
  - Resource Mgt & Web Services
  - Application Integration & Portals
  - Etc.

- Access Management
  - Federated Authentication
  - Account Restrictions
  - Secure Logging & Auditing
  - Monitoring
  - Notifications

- Identity Management
  - Role-based Admin.
  - Delegation
  - Workflow
  - Self Service
  - Triggers
  - Scheduling
  - Policy Lifecycle Mgmt.

- Identity
  - Integrated Identity

Novell Nsure
III. What are the Building Blocks of Identity and Access Management?

*Build on the right “Platform”*

Layer II: Manage your identities

- **Delegated / Role-based Administration**
  - The Security on the ID-Vault must allow to limit for Self and Group management, by Scope & Attributes
    (eg: be Admin, but only for the “Tel nr” of the BRU users)

- **Stealth mode**
  - Platform/database Admins still use their native consoles
  - Minimize the need for administrative console on the ID-Vault

- **Flexible Solution**
  - What if people move? (job/role change in HR?)
  - What if Policies Change?
  - and Authoritative Datasources?
Quick Win: Employee Self Administration

Employees can update some of their own identity data, like their GSM number or Car License plate.
III. What are the Building Blocks of Identity and Access Management?

*Build on the right “Platform”*

Layer III: Authentication, Authorization and logging
III. What are the Building Blocks of Identity and Access Management?

Build on the right “Platform”

Layer III: Access Control Management

- Select an Identity Vault that allows for strong authentication out of the box
  - token, RADIUS, Certificate, eID
- Federated Authentication (SSO with trusted partner)
  - SAML (Liberty Alliance), or WWW-Security
  - upcoming standard
- Logging / Alerting
  - Integrate with Corporate Logging / Alerting (SNMP)
  - Non-repudiation
- Account Restrictions
  - Intruder Detection
  - temporary suspending + auto reactivate
III. What are the Building Blocks of Identity and Access Management?

The need for a “Platform” AND “Solutions”

Layer IV: The Solutions

Secure Identity Management

Identity Driven Solutions
- SSO & Password Management
- User-Provisioning
- Web Access Control & SSO
- Resource Mgt & Web Services
- Application Integration & Portals
- Etc.

Access Management
- Federated Authentication
- Account Restrictions
- Secure Logging & Auditing
- Monitoring
- Notifications

Identity Management
- Role-based Admin.
- Delegation
- Workflow
- Self Service
- Triggers
- Scheduling
- Policy Lifecycle Mgmt.

Identity
- Integrated Identity
IV. Identity and Access Management Solutions

a. Novell SecureLogin: Solve the passwords nightmare
IV. Identity and Access Management Solutions

a. Novell SecureLogin: Solve the passwords nightmare
IV. Identity and Access Management Solutions

Login experience before Novell SecureLogin

1) Launch Application
2) Credential Challenge
3) Provide Credentials
4) Application Starts

Login ID: frank
Password:*******

Application
Client Workstation
Login experience with Novell SecureLogin

1) Authenticate to eDirectory
2) Launch Application
3) Credential Challenge
4) NSL Requests Secret from eDirectory
5) NSL Receives Secret from eDirectory, Supplies it to the Application

IV. Identity and Access Management Solutions

Login experience with Novell SecureLogin
IV. Identity and Access Management Solutions


Secure storage of passwords, opened by strong user authentication

- windows app
- browser App
- mainframe (terminal emulation AS/400, MVS, S390, …)
- thin client
- In house applications
- Java Applications
- API set and scripting

No Application Changes Required
IV. Identity and Access Management Solutions

a. Novell Secure Login: Enforce strong authentication to any application

- Password or Biometric

- Biometric and Smart Card

- Password and Biometric and Smart Card

- Something Else

Multifactor Authentication
IV. Identity and Access Management Solutions

a. **Novell SecureLogin**: *Solve the passwords nightmare*

Easy to Set Up Applications

- Auto-detection with Wizard for simple integration tasks
  - This is all you need 95%+ of the time
- Advanced configuration tool for complex tasks

Easy to Administer

- Single point of administration for organization-wide deployment & configuration
- Administrator sets overriding options for configuration
- SNMP Monitoring of login events and performance
- Separation of SSO Administration from IT Administration
IV. Identity and Access Management Solutions

a. **Novell SecureLogin**

*The Passwords Nightmare solved*
IV. Identity and Access Management Solutions

b. Novell Identity Manager: Identity Provisioning
IV. Identity and Access Management Solutions

b. **Novell Identity Manager**: The Zero day start project

Full systems support in Day One instead of in two weeks

-- Information entered once and synchronized across all systems
-- 70% reduction in administration costs
Novell, Before Zero Day Start
managing access to 168 applications, one-by-one
Employee provisioning streamlines business processes

Zero Day Start: making business more productive, more secure, more competitive....
IV. Identity and Access Management Solutions

b. Novell Identity Manager: Integrated Identities
Creating a complete identity from multiple authoritative sources

Enterprise Identity

Name: Julie Smith
DOB: 27 - July - 1963
Salary: level 22
E-mail: jsmith@acme.com
Phone: 408.555.1234
Prefs: ✓ ✓ ✓ ✓ ✓

Identity and Access Management Policies Implemented and Distributed Reliably as System Rules

Policy

Portions of Identity Managed by Appropriate Groups

HR
Finance
IS&T
Web
PBX

Self-service portal

A Single Virtual Identity… for employees, customers, partners, suppliers, etc.
IV. Identity and Access Management Solutions

b. Novell Identity Manager: Admins remain in charge with their existing tools
### IV. Identity and Access Management Solutions

#### b. Novell Identity Manager: Systems we connect

<table>
<thead>
<tr>
<th>eDirectory</th>
<th>Border Manager</th>
<th>DB2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>iChain</td>
<td>Informix</td>
</tr>
<tr>
<td>NT Domains</td>
<td>ZENworks</td>
<td>NIS +</td>
</tr>
<tr>
<td>NIS</td>
<td>Secure Login</td>
<td>/etc/passwd</td>
</tr>
<tr>
<td>Exchange</td>
<td>SunOne</td>
<td>AIX</td>
</tr>
<tr>
<td>GroupWise</td>
<td>iPlanet</td>
<td>Red Hat</td>
</tr>
<tr>
<td>Notes</td>
<td>Secureway</td>
<td>SuSE</td>
</tr>
<tr>
<td>LDAP</td>
<td>Critical Path</td>
<td>Solaris</td>
</tr>
<tr>
<td>Text</td>
<td>OID</td>
<td>Debian</td>
</tr>
<tr>
<td>JDBC</td>
<td>DirX</td>
<td>x.500</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>Oracle</td>
<td>Banner</td>
</tr>
<tr>
<td>SAP HR</td>
<td>Sybase</td>
<td>Oracle HR</td>
</tr>
<tr>
<td>Websphere MQ</td>
<td>MySQL</td>
<td>Cisco VoIP</td>
</tr>
<tr>
<td>SIF</td>
<td>MSSQL</td>
<td>RSA ACE</td>
</tr>
</tbody>
</table>

- Radius
- Oracle Financials
- Netegrity
- RACF
- ACF/2
- HP UX
- Tibco
- WebLogic
- JD Edwards
- In-Join
- Policy Director
- eTrust
- DSML
Layer IV : The Solutions

- **User Provisioning**
  - Zero Day Start / Zero Day Stop
  - Minimal impact on normal operations
  - Existing Administrators continue to work with existing management consoles (but benefit from the work of the others)
  - New employee with job/role created at HR
    - Provisioned with certain attributes in Identity Vault
    - Provisioned with certain rights on applications/devices/buildings
    - Applications are dispatched to the workstation (Need *Identity Based Software Deployment Solution*)
  - But also : *change of role* and termination

This can only work thanks to the underlying layers
IV. Identity and Access Management Solutions

b. Novell Identity Manager : Summary

Layer IV : The Solutions

• User Provisioning
  - Zero Day Start / Zero Day Stop
  - Minimal impact on normal operations
  - Existing Administrators continue to work with existing management consoles (but benefit from the work of the others)
  - New employee with job/role created at HR
    - Provisioned with certain attributes in Identity Vault
    - Provisioned with certain rights on applications/devices/buildings
    - Applications are dispatched to the workstation (Need Identity Based Software Deployment Solution)
  - But also : change of role and termination

This can only work thanks to the underlying layers
IV. Identity and Access Management Solutions

c. Web Access Management: What is the problem?

Issues when creating a Secure Web infrastructure:

- Direct Access to Web Servers (increase possibility of hacking)
- Multiple User Identities (no single sign on)
- Need to install SSL services on each web server
- Need to change links in HTML content from HTTP to HTTPS
- Many different Web Server Technologies
IV. Identity and Access Management Solutions

c. Web Access Management: The Novell Solution

Features of iChain:

- Single Authentication Point
- Provides Web Single Sign On (headers and Form Fill) - (can also simulate Netegrity SiteMinder)
- Sends Personalized content to applications
- Rewrites HTML data (completely hide internal DNS infrastructure)
- Dynamically encrypts content as it passes through proxy
- Single SSL Certificate can be used for all internal web sites (proxy based)
- No change to HTML content
- No change to applications authentication process
- Secures all HTTP servers (no conflicts with ISAPI services)
- Remove Direct Access to Web Servers
IV. Identity and Access Management Solutions

c. Web Access Management: *iChain, how does it work?*

1. Authentication - Who are you?
2. Access Control - What do you have access to?
3. Single Sign On
4. OLAC (Personalization)
5. Data Confidentiality

![Diagram of web access management with iChain](image_url)
IV. Identity and Access Management Solutions

c. Identity Based Resource Management: Novell ZenWorks
IV. Identity and Access Management Solutions

c. Identity Based Resource Management: Novell ZenWorks

Complete IT resource management for enterprise-wide efficiency
IV. Identity and Access Management Solutions

c. Identity Based Resource Management: Novell ZenWorks manages your Windows environment

- No enterprise-wide distribution of Novell client required
- Runs on Windows (and NetWare and also supports Linux and Solaris servers)
- Leading meta-directory solution included, Novell eDirectory
- Ability to integrate with Active Directory provided in the box
IV. Identity and Access Management Solutions

c. Identity Based Resource Management: The ZEN experience

Three fundamental concepts have made ZENworks the industry leader:

- Policy-enabled management
- Managing the complete workstation lifecycle
- Enabling the digital identity
Policy-enabled Management
The Power

- Polices make **one-to-many administration** possible

- Novell ZENworks builds all of its policy-enabled intelligence into the directory

- Using the directory **secures** management and allows re-use of business information

- **Policies are crucial** for making reliable deployments, rollouts, and other mass changes to your network

**Temp Worker Policy**
- No C: access
- No application installation
- No registry editing tools
- Force standard wallpaper
- Silent-mode remote control
- Access to email application from 8:00 - 5:00
• The Digital Persona includes:
  - Personalized preferences and settings (roaming profile)
  - Desktop, network and web applications; personalized for the end user
  - Configuration-managed Desktop, including lockdowns based on Windows policies
  - Local user account, dynamically created from eDirectory (DLU=Dynamic Local User)
The Digital Persona includes:

- Personalized preferences and settings (roaming profile)
- Desktop, network and web applications; personalized for the end user
- Configuration-managed Desktop, including lockdowns based on Windows policies
- Local user account, dynamically created from eDirectory (DLU=Dynamic Local User)
Remember:
If you want your Identity Management Solutions to fly....

You need a fully INTEGRATED STACK
V. Return on Investment
V. Return on Investment

*Return from Business Facilitation*
V. Return on Investment

Return from Increased Security/Risk Avoidance

Your business

Security policies

Nsure

Employees

Partners

B2B

Customers

Finance

Marketing

Sales

Customer service

One time

Automatic

Across all systems

Eliminates mistakes
V. Return on Investment

Return from Operational Cost Reduction
V. Return on Investment

Return from Regulatory Compliance

Customer

Your business

Audit
V. Return on Investment

Return from Productivity Gains

New employees receive access and resources quickly and automatically, based on roles and responsibilities.
V. Return on Investment

Return from Increased Customer Satisfaction
VI. Customer References
Gemeente Den Haag - One Net Vision enables open eGovernment

- 450,000 Residents provided with secure access to tax valuation criteria and single sign-on to other government services

**Benefits:**
- Reduce number of complaints over payment of municipal taxes
- Faster response to tax assessments and receipt of payments
- Greater openness, interaction and understanding of residents
Goal: Reduce procurement costs by 25% over the next five years through integrated processes.

Build trust partnerships with 10,000 suppliers through secure Internet access to procurement systems.
Characteristics:
- Worldwide, nomadic workforce
- 70,000 employees
- Complex variety of applications, platforms

Specific goals:
- Secure employee access worldwide
- Reduce directory administration costs for multiple applications
- Personalize application delivery
VII. Listen to the Analysts
Gartner’s Magic Quadrant for Metadirectory Products

As of September 2003

Source: Gartner Research (September 2003)
Identity and Access Management:
A full stack of integrated modules

Remember to look for a suite that offers you a full stack of integrated modules:

- your Directory is your backbone, be sure it is “Worldclass”
- some solutions focus too much on LDAP but are weak on the Meta- and Solutions-side
- some solutions run only on one platform, tend to “tweak” the standards and “lock you in”
- some solutions are composed of parts thru acquisitions 2 years ago and still do not integrate
- some nice solutions miss the underlying stack and work best on paper

And now you can tell...