Imagine there are no passwords

HIC’09, Canberra, Australia
Challenges for Health IT systems security

- Patients expect their personal health data to be handled securely
- Clinicians require improved efficiency interacting with health IT systems
- Organizations expect greater visibility into access of electronic health information
Health IT systems are complex

- Many independent applications
  - with their own authentication schemes
  - with their own audit mechanism

- Heterogeneous application delivery platforms
  - Mainframe, Windows, Java, web applications
  - Heritage applications still in use and providing value

- Stronger security policy can’t be easily applied across all of these systems

- Most clinician access is provided through a desktop environment
  - But there are current and emerging requirements for levels of remote access and mobility
Clinicians are constrained today

- Clinicians must keep changing their passwords
  - Example: 1800 password reset calls per month from a public sector health care organization

- Each clinician requires a different password per application

- Application policy requires that sessions time out

- Time and motion studies show up to 10% of clinicians time spent logging onto systems

- No session mobility for clinicians
Doesn’t NASH provide a solution?

- NASH delivers a strong provider authentication system (NASH) using key capabilities for E-Health services
  - Smartcards for healthcare professionals
  - Digital certificates for devices
  - Enable trusted authentication, digital signing, encryption

- NASH does not aim to address the following problems:
  - Single Sign-on to clinical applications in use today
  - The need to perform audit of application access for all users
  - Clinician’ Session and context mobility
  - On boarding challenges associated with enabling new users
How can we address these challenges today?

- Make the desktop the authentication authority for internal users
  - Introduce NASH authentication at the desktop (second factor)
  - Every clinician authenticates to the desktop with smartcard

- Leverage Single Sign-on technologies
  - Remove the need for clinicians’ application passwords
  - Use trust and federation to propagate identity
  - Automate the start-up of applications based on role

- Introduce identity governance technologies
  - Automically provision users on applications prior to employment

- Minimize impact on existing infrastructure

- Audit application access from the desktop
Efficiency through Single Sign-on automation
Fast enablement of transient employees

Identity Governance using Policy Management

Applications
Entitlement
Application Roles

Data
Unstructured Data
Structured Data

People
Business Roles
Users

Monitoring
User activity monitoring and conformance to policy and regulations
Support clinician mobility and consolidate
Case Study: An Integrated Healthcare Network

Company
- Integrated delivery network of 16-facilities in central California
- Over 7,800 employees

Problem
- Regulatory compliance requirements (HIPAA)
- Securing workstations shared by multiple users
- Strong user resistance to new security policies

Solution
- Implement IBM Tivoli Identity and Access solution

Impact
- Immediate compliance to HIPAA regulations
- Dramatic improvement in user acceptance
- Ability to provide user centric access logs to applications
- Leverage existing access card investment to provide rapid secure access

Deliver improved patient outcomes today

- Improve productivity and increase efficiency
  - Build automation (identity and SSO) into your existing solution

- Introduce identity governance
  - Automate provisioning and de-provisioning of users

- NASH is developing standardised authentication schemes for application delivery platforms
  - Integrate these schemes into the desktop
  - This supports introduction of stronger authentication schemes for access to patient records
  - Consider mobility solutions that support flexible authentication schemes
Chris Hockings  
Senior Security Specialist

IBM Australia Limited  
Level 11, Seabank  
12 Marine Parade  
Southport Qld 4215

Tel  +61-7 5552 4012  
Fax  +61-7 5571 0420  
Mobile  +61-402 893 662  
hockings@au1.ibm.com