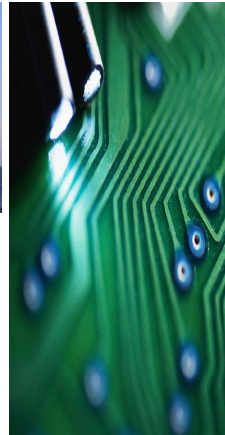




# IT128 Single Sign-On: A Success Story

## Implementing Strong Identity at Chevron



**2006 PIMA International Leadership Conference**

**Edmund Yee**

**Chevron ITC**

**IT Infrastructure Strategic Research Manager**

# Agenda

- Background on Chevron
- Role of Identity at Chevron
- Top 5 business drivers for stronger Identity
- Requirements for strong Identity
- Integrated solution
- Global deployment
- Top 10 Lessons learned
- Sample Video
- Q&A



# Chevron Corporation

## 2<sup>nd</sup> largest U.S. Energy Company

- 55,000 employees worldwide
- Over \$190 Billion in revenues
- 4th largest integrated energy company in the world
- Operations in over 180 countries
  - Producing and transporting crude oil and natural gas
  - Refining, marketing, and distributing fuels & other energy products.

# Chevron IT Landscape

- 4 Major Data Centers
- Predominately Microsoft Infrastructure
  - Active Directory and Microsoft Servers
  - Standard Windows XP Desktop/Notebook
- Technical Computing – Seismic Interpretation
  - LINUX for Technical desktop
  - LINUX Cluster servers
- 2-factor Network Authentication
- Major Enterprise Applications - SAP, JDE (Oracle)

# Role of Identity at Chevron

## ■ Types of users

- Employees – 55,000
- Contractors – 20,000
- 3<sup>rd</sup> Parties – 5,000
- Joint Ventures – 5,000

## ■ Kinds of identities

- User IDs
- Administrative IDs
- Device IDs – Networks
- Service IDs - Applications

## ■ End Points

- LAN/WAN – Local, Sat, slow links
- Wireless – 802.x, PDAs
- Remote – VPN & Citrix
- 3<sup>rd</sup> Parties - Partnerships

## ■ Business processes relying on identity

- LoB Applications – SAP, Oracle, Seismic, etc...
- Desktop Access – Windows & LINUX SignOn
- Device Access – Network device management

## Top 5 Business Drivers

- M & A – unify physical & logical access into a single corporate identity card - SmartBadge
- Penetration & vulnerability audit results
  - Higher level of Security
  - Chevron Board's Audit Committee created an edict
- Proactive role in legislation & regulatory trends – Homeland Security
- Outsourcing – IT outsourcing of Mission Critical Applications (SAP, JDE...)
- Cost reduction
  - #1 Helpdesk problem: password management

# Strong Identity Requirements

- Single Workflow Process - Quick turn-around to provision/de-provision IDs
- Easy to use
- Highly secure - 2-factor authentication for network access (no passwords)
- Cost effective global solution
- Enterprise application support
- Support for encryption and digital signatures
- 3<sup>rd</sup> Party support
- Solution for remote/challenging environments
- Single sign-on (ESSO and Web SSO)

# Integrated Solution: Public Key Infrastructure (PKI)

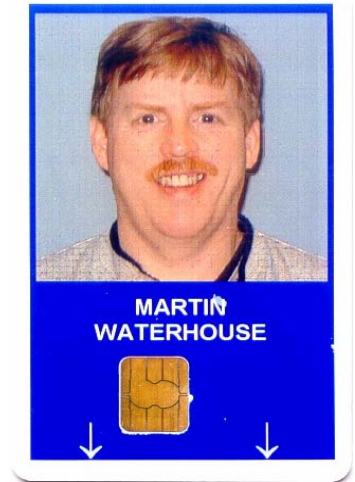
- Implement a standardized global infrastructure that allows for certificate based authentication, encryption and non-repudiation .
- Benefits of the standardized PKI infrastructure include:
  - Globally availability with standard desktop
  - Secure Network Logons, messaging encryption and Applications authentication
  - Non-repudiation with digital signature
- What makes this possible?
  - Windows Sever 2003 PKI with Hardware security modules
  - CP/CPS
  - Web Trust for CA standards
  - Executive security governance council



# Integrated Solution: SmartBadge



- SmartBadge: Corporate Identity Card providing physical and IT security. (Smartcard with HID antenna)
- Benefits of the SmartBadge include:
  - Secure, two factor authentication
    - 1) Something you have – **Badge** and
    - 2) Something you know – **PIN**
  - Embedded brute force protection
  - Highly secure and user friendly self-service
  - Portable, secure and multipurpose
  - Integrated application security
- What makes this possible?
  - Centralize facility access control
  - Directory and Provisioning system
  - Smartcards and smartcard readers
  - Feature-rich Card Management System integrated with Active Directory and Windows 2003 PKI
  - Global XP standard desktops and notebooks with smartcard middleware
  - Integrated Enterprise SSO (Password Management Tool)

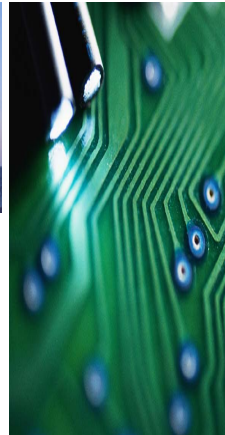


# Deployment Milestones

1. Issued 75,000 Smart cards for physical access (*Phase #1*)
2. Standardized and Integrated a single global physical access system
3. Integrated a Multi-tier Microsoft 2003 PKI
4. Integrated a Feature-rich Card Management System (CMS)
5. Deployed smartcard reader hardware
6. Activated 60,000 users for logical access using regional deployment coordinators (*Phase #2*)
7. Enabled digital signatures and encryption for office documents and emails
8. Defined and deployed Remote Access management with 2-factor Authentication
9. Integrated Enterprise Single Sign-On with smartcards
10. Deployed password enforcement/elimination tools
11. Extended smartcard logon beyond windows environment



# Implementing Strong Identity at Chevron



## Top 10 Lesson Learned

## Don't do it alone!

Strong authentication projects are complex and involve:

- Various technologies
  - Public Key Infrastructure (PKI), CP, CPS, Digital signing...
  - Physical access systems, door readers, card printers, biometrics...
  - Smartcards and readers, middleware, Card Management System...
  - Directories, Automatic Provisioning
  - Application Integration – applications that utilize AD authentication
  - Other supporting Apps: password management, VPN, secure email, hard drive encryption, File encryption, secure web...
- Various company divisions: HR, security, IT, Financial, Business Units...



### Recommendations:

- Talk to people from other companies who have deployed these technology successfully
  - Obstacle: security is confidential
- Strong authentication is a core infrastructure components – affect many systems
- Consult with Identity Management experts with hands-on experience
- Example: consider outsourcing PKI

## Don't neglect compliance with other projects!

### Identity & Access Management is Infrastructure

- Infrastructure components are linked
  - Examples of projects
    - ▶ Email server changes (e.g.: MS Exchange)
    - ▶ Directory services (e.g.: extensions)
    - ▶ Remote access (e.g.: VPN)
    - ▶ WiFi



### Recommendations

- View Smartcard project within a larger program
- Interact and communicate with other projects
- Define common security goals
- Update security standards (Enterprise Security Architectural Standards) as soon as possible

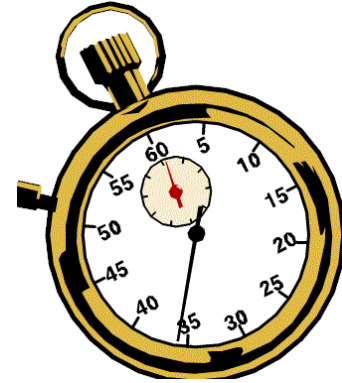
## Don't rush it!

Smartcard deployment projects consistently take more time than planned:

- Smartcards or Readers don't arrive on time
- Physical and Logical access projects are not in sync
- Pilot programs drag for months instead of weeks
- Processes definition and implementation lag behind technology

Recommendations:

- Lengthen your project plans
- Follow a phased approach – baby steps
- Follow up closely on hardware delivery timeframes
- Coordinate the physical and logical security projects



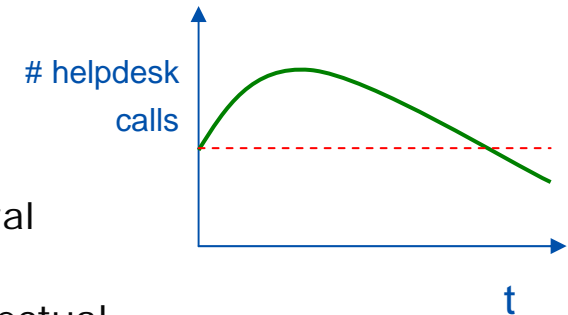
## Don't do it only for ROI!

Smartcard based employee badges are primarily for more security:

- ROI can be realized in:
  - Password management (Single Sign-On)
  - Combining physical access cards
  - Internal & external paperless transactions (digital signing)
  - Soft ROI or CINI (Cost If Not Invested) in Intellectual Property protection
- However pure financial justification is difficult
  - Benefits are not tangible
  - It requires many other changes in the organization with high costs (e.g.: digital signing)

### Recommendations:

- Set 'heightened security' as a primary goal of the project
  - Define measurable success rates for security



## Don't do it without the Chiefs!

Smartcard deployment has its ups and downs over a relatively long period of time:

- It requires acceptance from all categories of employees
  - Executives
  - HR
  - Managers
  - Staff
  - Contractors
  - Visitors

### Recommendations:

- Seek executive support and sponsorship early on
- Organize a 'governance model'
- Communicate regularly with the stake-holders including the Financials



## Don't overload it!

Adding more supporting applications/features to the smartcard eventually leads to better ROI:

- OS logon, email encryption and signing, password management tool, secure web, VPN, on-card One-Time-Password, physical access, biometrics, file encryption, electronic payment, healthcare record, automatic provisioning...
- However both managing many applets on card and managing many systems in the back-end can compromise the success of your project



## Recommendations:

- KISS (Keep It Short & Simple...) - baby steps and build on success
- Create reasonable roadmap and gradually add applications/features
- Do pilots with clear and measurable results

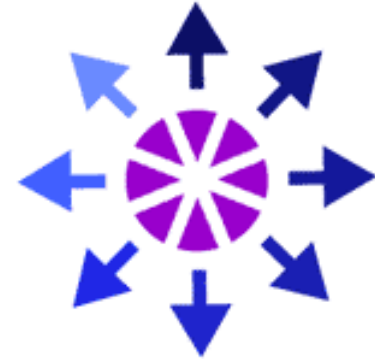
## Don't do everywhere at once!

Lessons learned from one location are valuable for other locations:

- Business rules specific to your company environment impact your deployments
- Some locations are more strategic than others

Recommendations:

- Create a 'swat' team that goes from location to location
- If using external help, demand same people be sent to different sites
- Use deployment coordinators
- Document lessons learned
- Carry out surveys in each location



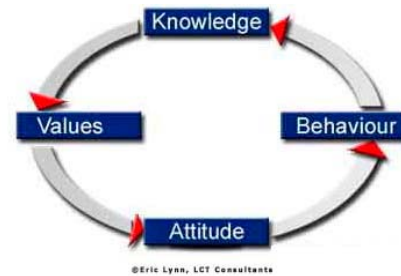
## Don't overlook culture change!

Inertia is strong especially when it comes to security:

- Difficult to convince everyone of benefits of security on a daily basis
- End-user convenience is relevant but sometimes clashes with security
  - New system must work at 99.9% or it leads to frustrations
- The transition is difficult
  - Many don't understand why they have to change habits
  - Techies find smart cards more 'cool' than others!

Recommendations:

- Spend time to develop detail change management program
- Executive training program
- Communicate, train, re-communicate, retrain!
- Define security goals as formal work objectives for managers and their teams



## Don't do it without a good C.M.S!

Card Management System (CMS) manages the life cycle of the smart card:

- Scenarios:
  - What are the workflows for card creation, initialization, personalization?
  - How to replace a lost card?
  - How to issue a temporary card?
  - How to unblock a card remotely?...
- Applet loading / updates
  - Applets and their personalization can be automatically updated on cards already deployed

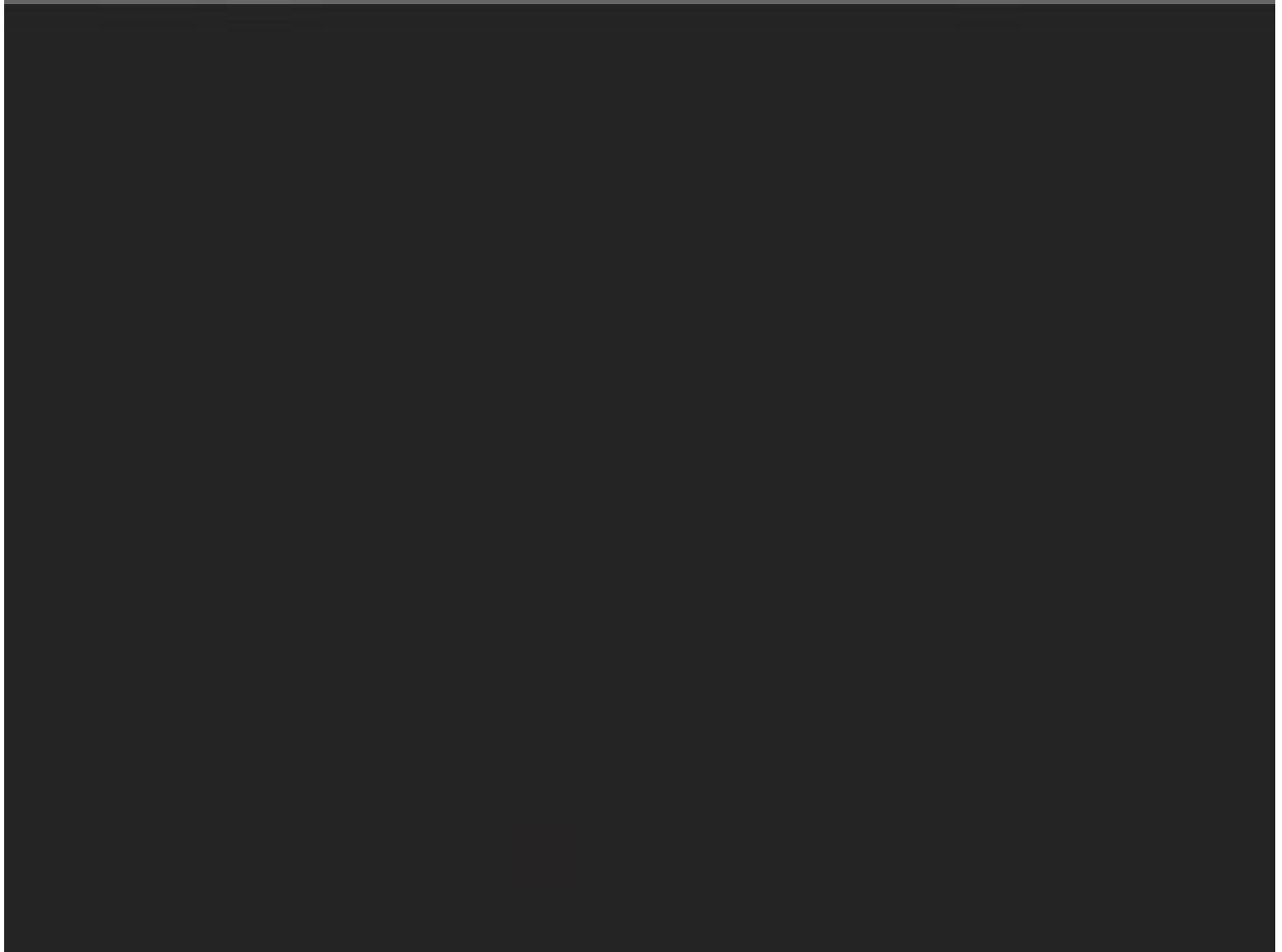
Recommendations:

- Pilot the CMS and make sure it covers all cases
- CMS must offer remote functions such as PIN reset and PIN unblock
- Challenge: maintain high level of security and convenience





# SmartBadge Video



# Questions

