



Charles Tostain & Emmanuel Fauconnier

Single Sign-On **Tivoli.** software

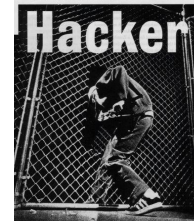
Simplifiez la vie de vos utilisateurs avec le SSO



**TENDANCES LOGICIELLES D'ÉTÉ 2008**

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

# IBM et Tivoli : Les enjeux de la sécurité informatique



## Périmètre Défensif



Offre ISS



### Périmètre défensif

Fermer la porte aux intrus avec:

- Firewalls
- Anti-Virus
- Détection d'intrusion, etc.

Mettre en oeuvre des mécanismes de protection des systèmes a toujours été une préoccupation importante des Responsables Informatiques

Une étude menée pour le compte d'IBM en 2006 indique que 70% des personnes interrogées considèrent que l'identification des failles de sécurité est un élément indispensable.



## La Sécurité

- ...Mais on estime que 75% des vols de données viennent de l'intérieur de l'entreprise
- ... les Entreprises sont beaucoup moins protégées...



Massive Insider Breach At DuPont  
A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706 more in the company's electronic library.

By Larry Greenemeier  
InformationWeek  
février 15, 2007 03:00 PM



The Delaware U.S. attorney on Thursday revealed a **massive insider data breach at chemicals company DuPont where a former scientist late last year pleaded guilty to trying to steal \$400 million worth of company trade secrets**. He now faces up to a decade in prison, a fine of \$250,000, and restitution when sentenced in March.

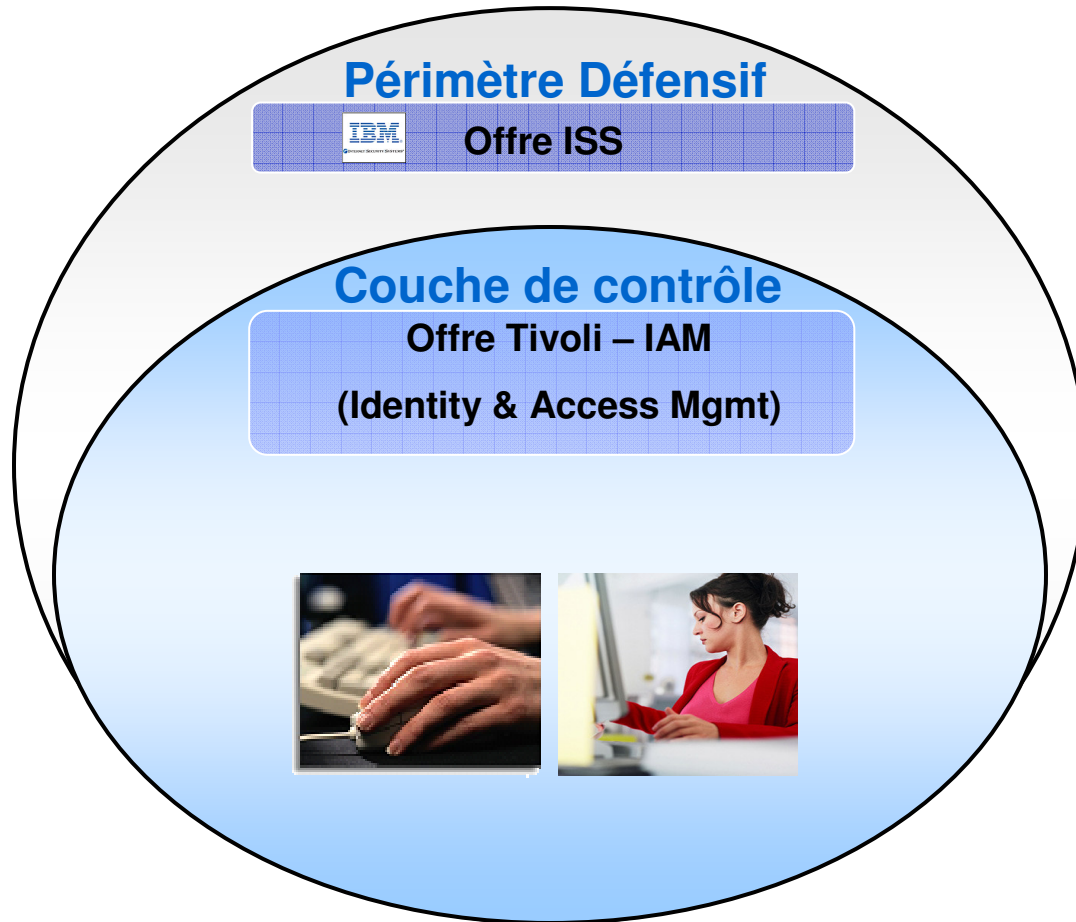
Gary Min worked as a research chemist for DuPont for 10 years before accepting a job with DuPont competitor Victrex in Asia in October 2005. Between August and December of that year, Min downloaded 22,000 sensitive documents and viewed 16,706 more in DuPont's electronic library, making him the most active user of that database in the company, according to prosecutors.

**75% of the 40 proprietary and confidential information thefts studied between 1996 and 2002 by Carnegie Mellon's CERT program in a July 2006 study were committed by current employees**, says Dawn Cappelli, a senior member of the technical staff at the CERT program at Carnegie Mellon's Software Engineering Institute.

**TENDANCES LOGICIELLES D'ÉTÉ 2008**

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

# IBM et Tivoli : les enjeux de la sécurité informatique



## Périmètre défensif

Fermer la porte aux intrus avec:

- Firewalls
- Anti-Virus
- Détection d'intrusion, etc.

## Couche de contrôle

- Qui peut entrer?
- Que peuvent-ils voir et faire?
- Accès liés aux rôles?
- Protection de la vie privée?



## Conformité et auditabilité



► Respect des règles à mettre en oeuvre

- Sarbanes-Oxley – Contrôles d'audit améliorés, protection des investisseurs

- Loi de sécurité Financière (LSF) : Contrôle interne du reporting financier et communication financière

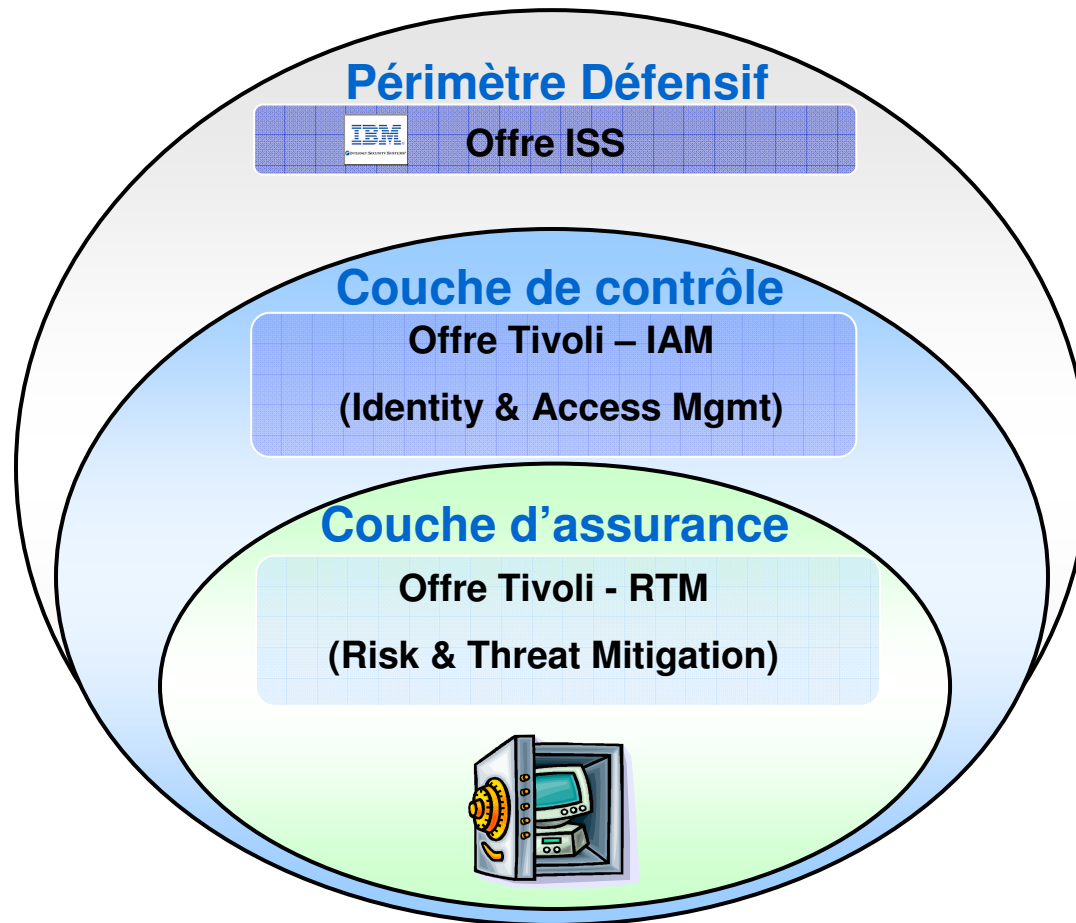
- PCI: Payment Card Industry: PCI définit des exigences en matière de sécurité des données des cartes bancaires.

- Bale II : Contrôle et gestion du risque

► Fournir les outils permettant d'éditer les rapports utiles aux auditeurs



## IBM et Tivoli : Une offre complète



### Périumètre défensif

Fermer la porte aux intrus avec:

- Firewalls
- Anti-Virus
- Détection d'intrusion, etc.

### Couche de contrôle

- Qui peut entrer?
- Que peuvent-ils voir et faire?
- Accès liés aux rôles?
- Protection de la vie privée?

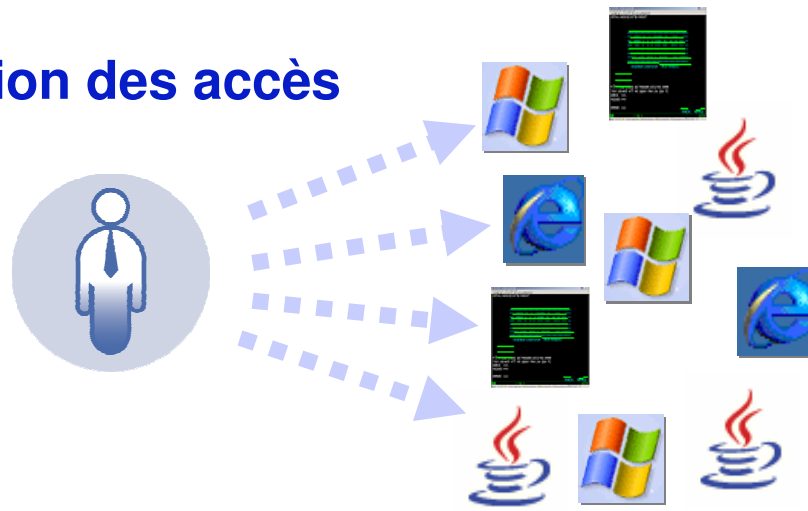
### Couche d'assurance

- Conformité aux réglementations?
- Rapports et auditabilité?
- Suis-je en situation de risque?
- Réponse aux événements de sécurité?

**TENDANCES LOGICIELLES D'ÉTÉ 2008**

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

## IAM: Quelques constats d'inefficacité dans la gestion des accès



Accès au SI pour un nouvel utilisateur (Provisioning)

**12 jours en moyenne pour créer les accès à un nouvel utilisateur**

Gestion des Utilisateurs

**20\$ par appel pour la réinitialisation des mots de passe**

Suppression des accès (Dé-provisioning)

**30 à 60% des comptes sont invalides**

Nouvelles applications

**Jusqu'à 30% du temps de développement sur le contrôle d'accès**



Solution de SSO **Tivoli.** software

**IBM Tivoli Access Manager for  
Enterprise Single Sign-On**



**TENDANCES LOGICIELLES D'ÉTÉ 2008**

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS



## IAM: Quelques constats

### Inefficacité dans la gestion des mots de passe

#### Règles de sécurité et réglementations

- ▶ Nécessité de respecter les nouvelles réglementations
- ▶ Les mots de passe doivent être difficiles à pirater



Mots de passe complexes  
Qui doivent être changés fréquemment

#### Résultat:

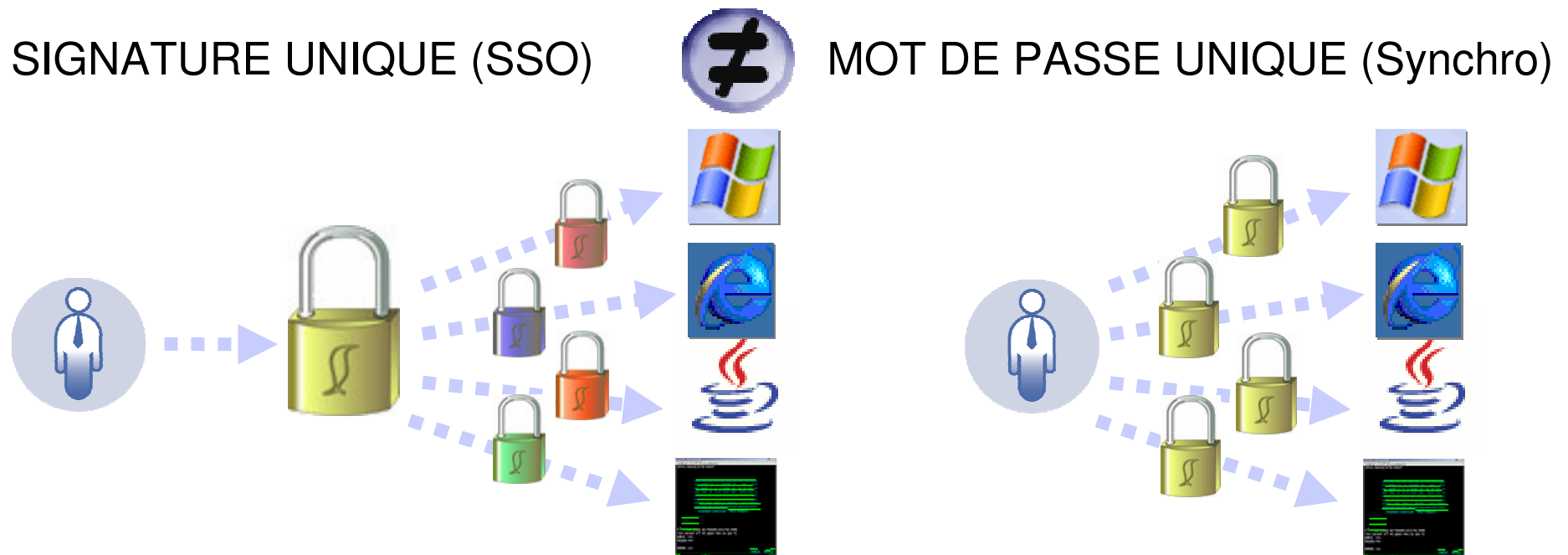
- Mécontentement & plaintes des utilisateurs
- Coût pour l'entreprise
  - ▶ Utilisateur bloqués, interruption de service
  - ▶ Coût élevé du support utilisateur
  - ▶ Perte de productivité
- Problèmes de Sécurité
  - ▶ Il est difficile de d'intégrer de l'authentification forte
  - ▶ Sécurité affaiblie par une mauvaise gestion des mots de passe.



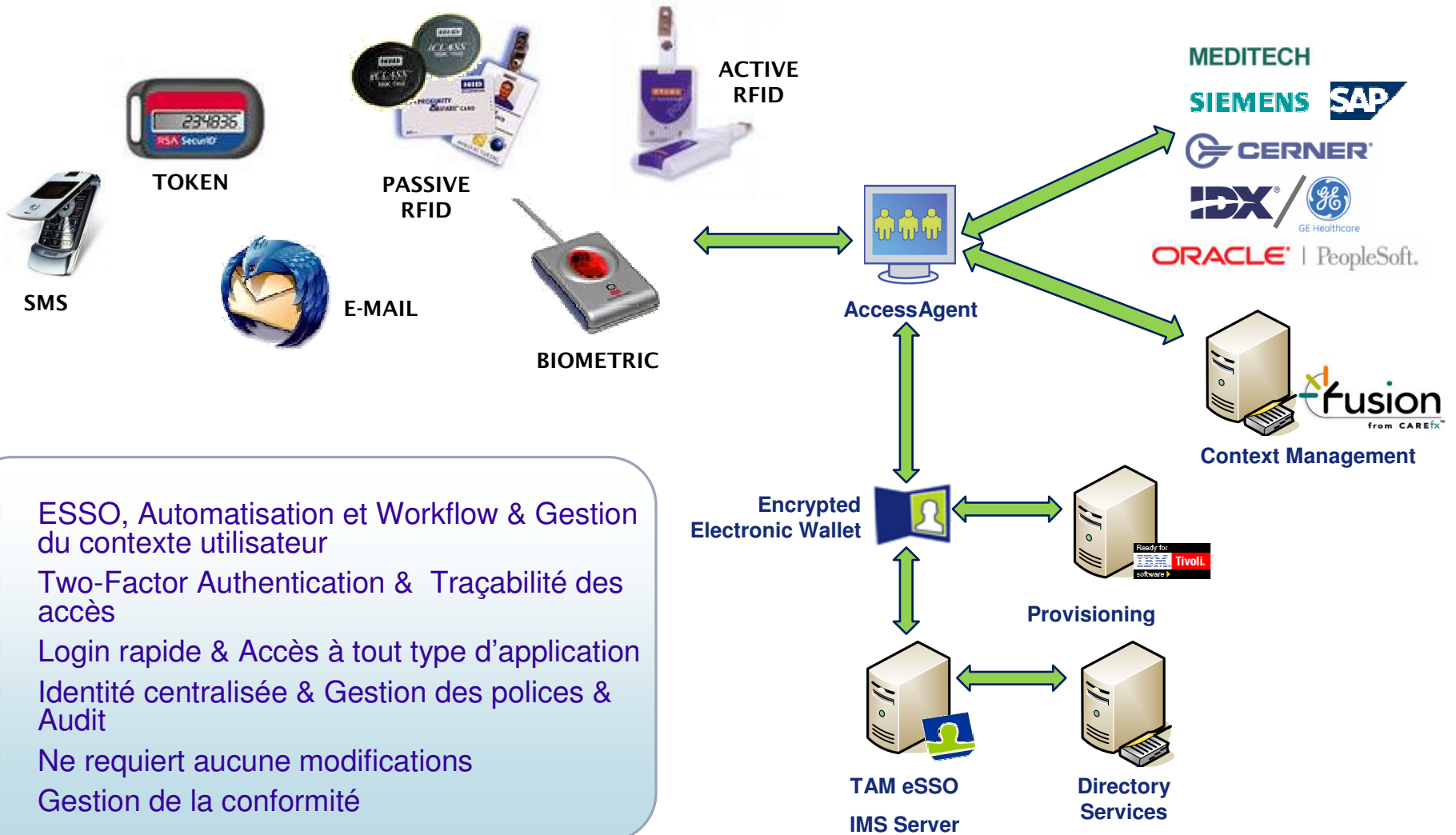
## SSO Entreprise ou Poste de Travail : SSO étendu

- Identifier les utilisateurs quand ils ont besoin d'accéder à une ressource système ou un réseau
- Utilisé comme base pour autoriser l'accès aux applications
- S'insère entre l'utilisateur et ce qu'il fait

**A ne pas confondre !**



# TAM for eSSO

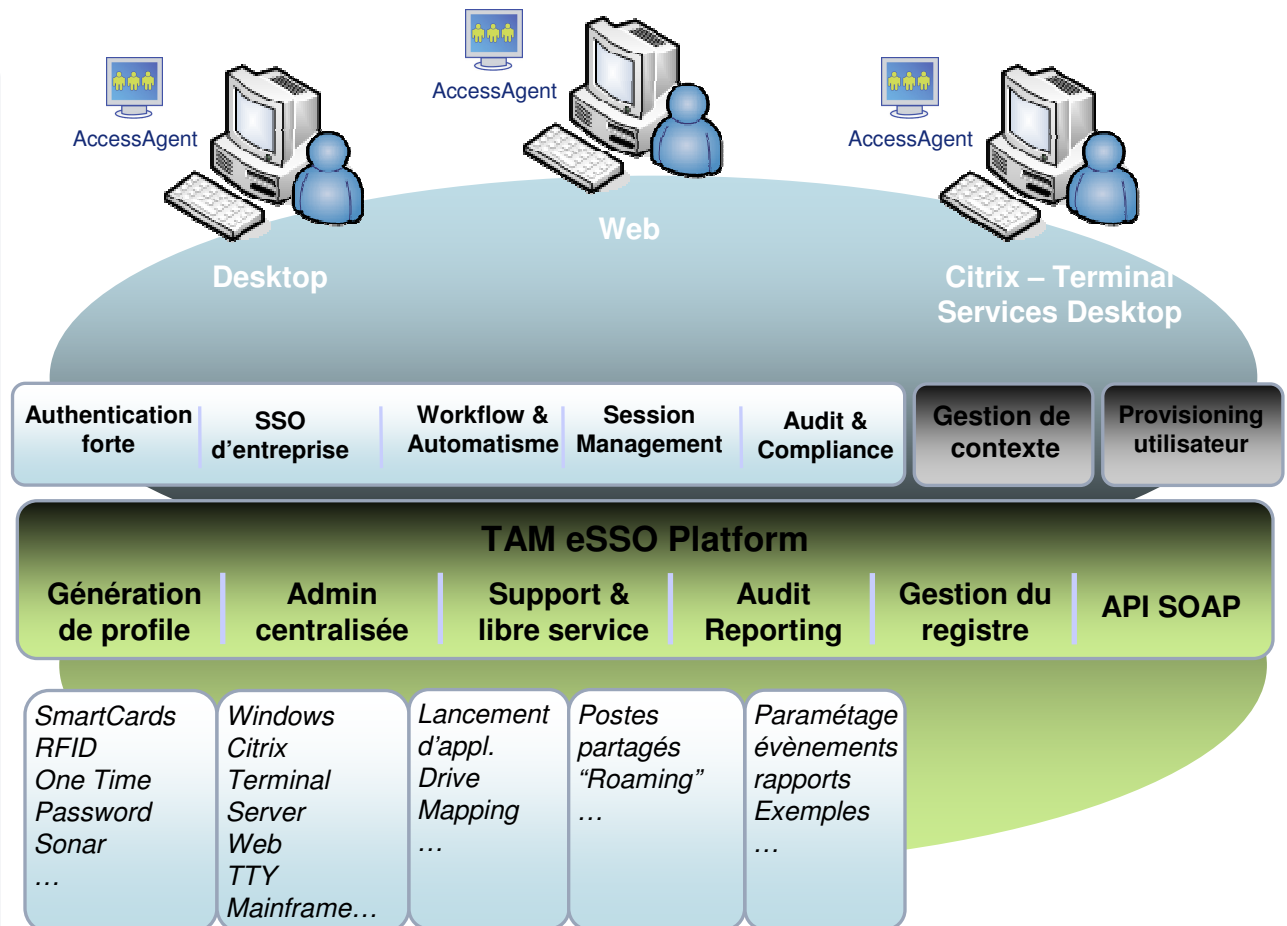


- ESSO, Automatisation et Workflow & Gestion du contexte utilisateur
- Two-Factor Authentication & Traçabilité des accès
- Login rapide & Accès à tout type d'application
- Identité centralisée & Gestion des polices & Audit
- Ne requiert aucune modifications
- Gestion de la conformité

# Un support étendu du SSO pour tout type de terminaux

## TAM eSSO:

- Simplifie l'expérience utilisateur et améliore la productivité en éliminant le besoin de se souvenir de multiple identité et mot de passe
- Facilite la mise en oeuvre de la compliance avec les fonctionnalités de traçabilité et en collectant les accès
- Améliore la sécurité en éliminant les mot de passe faible et en intégrant des facteurs d'authentification fort
- Réduit le recours au Help Desk en diminuant la demande de réinitialisation de mot de passe



\* Integrated Management System

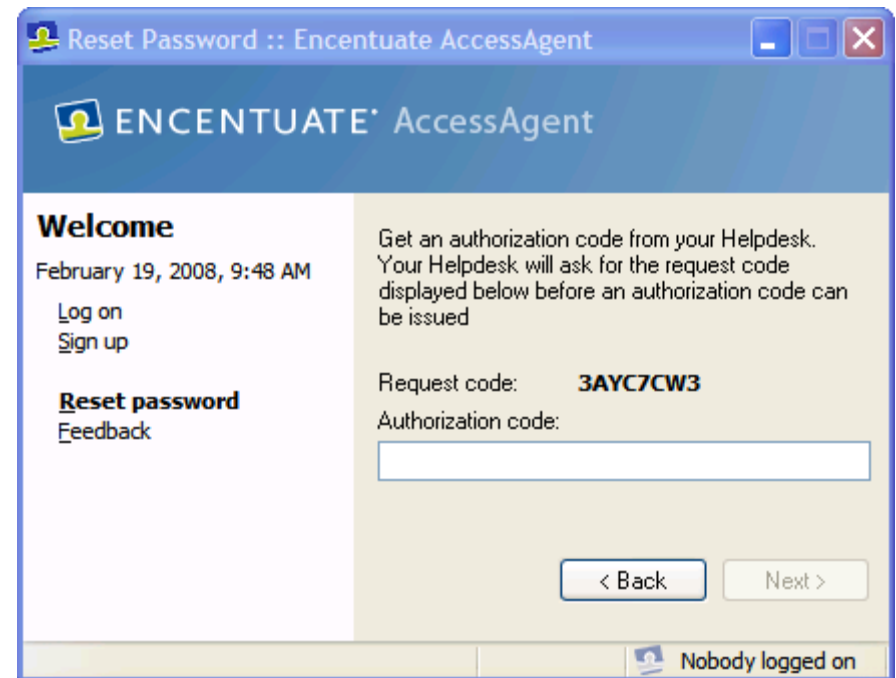


## Autres fonctions: Self-service Reset

- Self-service password reset
- Bypass de l'authentification de second niveau

## Autres fonctions: Reset offline

- Reset du mot de passe pour les utilisateurs mobiles non connectés



## Autres fonctions: Cas de perte de l'authentification forte

- Fourniture d'un code d'autorisation temporaire par le help desk
- (cas de perte d'un badge RFID, token, OTP, etc...)

Log On :: Encentuate AccessAgent

ENCENTUATE AccessAgent

**Welcome**  
February 19, 2008, 9:46 AM

[Log on](#)  
[Sign up](#)

[Reset password](#)  
[Feedback](#)

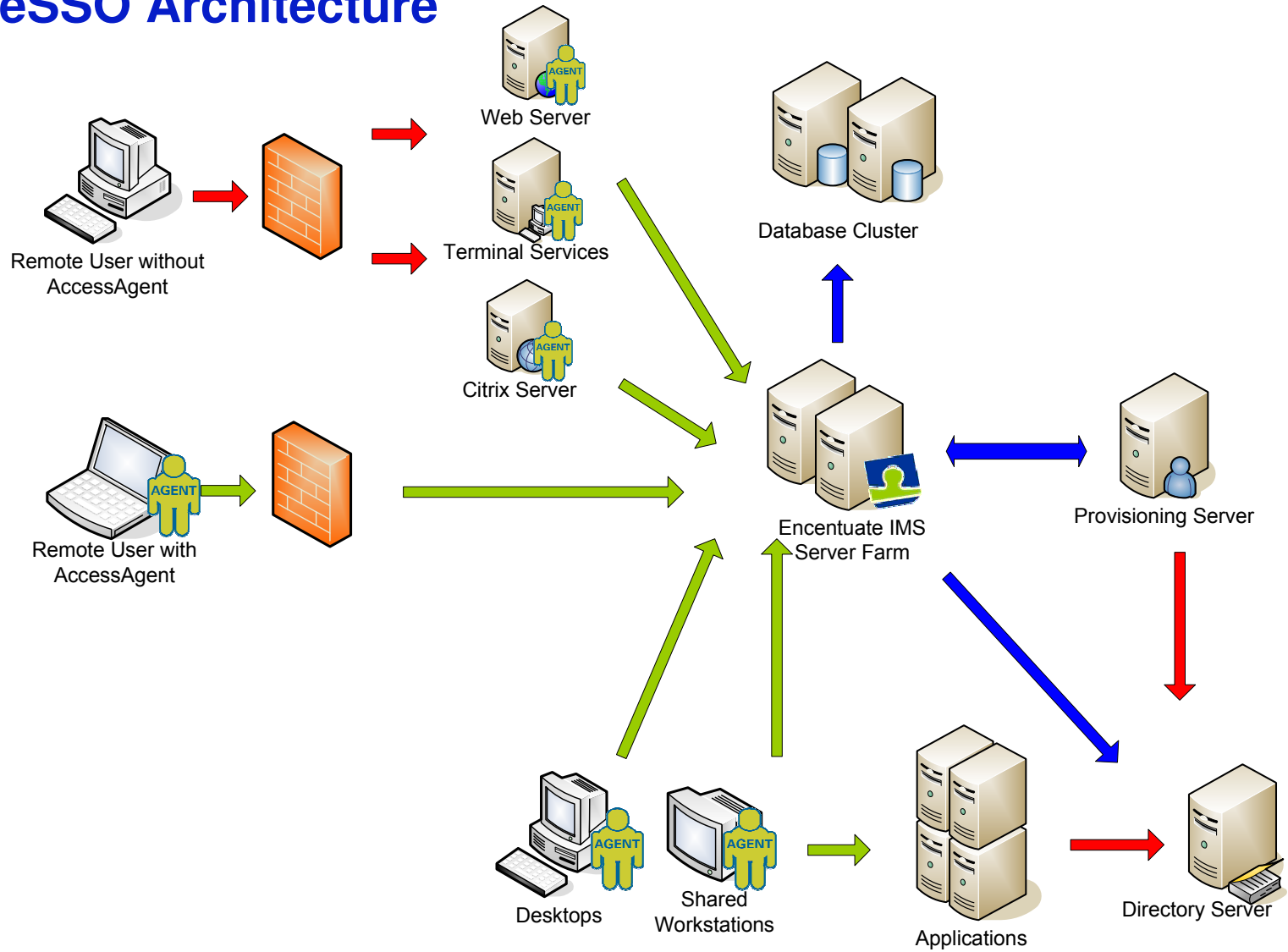
Enter the authorization code provided by your Helpdesk.

Authorization code:

Finish

Nobody logged on

# TAM eSSO Architecture





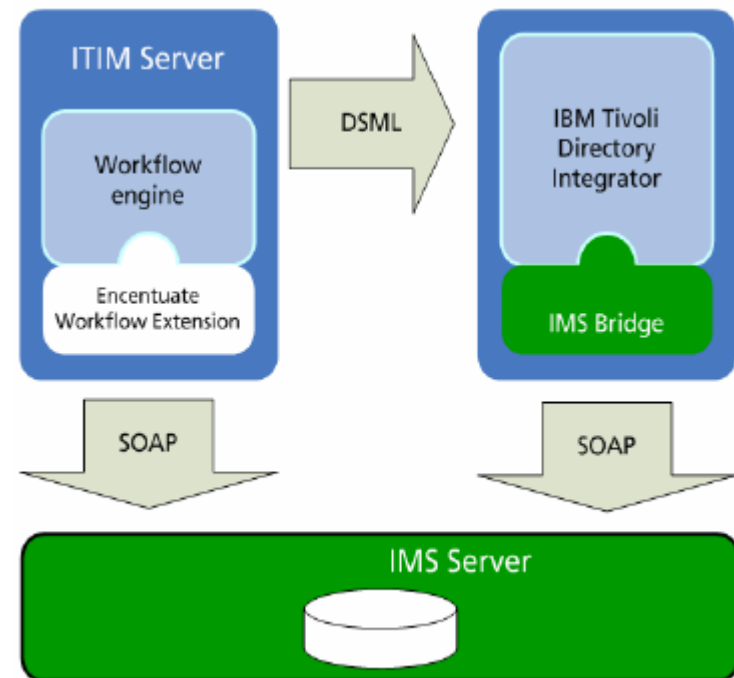


- A4 HealthMatics
- ABS
- AccessLine
- AccessMyCMC
- Activconsole
- ActiveX Test App
- AdminPass
- AH INTRANET
- AION
- Alert32
- AlertMonitor
- Am\_nt
- API Software
- API-Report Express
- ASK IT
- Aurora
- Bcscons
- Blue Cross CA
- Blue Shield
- Blue Shield Subscriber
- BudgetAdvisor
- Busobj
- Caliber RM
- CallLog
- Callog32
- CapitalAdvisor
- Captura
- Careman
- CareManager
- CBISA-WebEntry
- Centicity RIS Technologist
- Centicity RIS Equipment Manager
- Centicity RIS Key Word Search
- Centicity RIS
- Mammography Tracking
- Centicity RIS Order Management
- Centicity RIS Radiology
- Centicity RIS Report Browser
- Centricity RIS Scheduling
- Centricity RIS Supply Management
- Centricity-PACS
- Centricity-Portal
- Centricity-RIS
- Centricity-Web
- CERME
- Cerner Millennium
- Certified Mail
- Chargemaster
- Chart Review
- ChartMaxx
- CHB Network Drives
- CHB Web Application
- Chemotherapy Order Entry
- CHMenu Web
- Cigna
- Cigna Subscriber
- Cirius
- Cirius\_Reports
- Cisco VPN Client
- Cisco VPN eToken
- Citrix
- Citrix ICA Client
- Citrix Nfuse
- Clinical Workstation
- ClinicalBrowser
- CMS Supervisor
- CodeCorrect
- Cognos
- Cognos Impromptu
- Computation
- Connect32
- Content Manager
- Cplgv
- CPRS
- Cprtm
- Cpsecuremotepw
- CPSS Enquiry
- CPSS Production
- Cpstat
- Cpusemonitor
- Cpusemonitor
- Craneware
- CRM
- CWEB
- DBS.com
- DCHS Access
- Dchsnet
- DDE
- Designer
- DSG Support
- DSG-GUI
- Eadmin32
- e-Claims
- Econolink2000
- ED Tracking Board
- (PCView)
- EDOC Writer
- EDWeb
- eGate
- Electronic Patient Folder
- EMDS
- Empower
- EMR
- EMR\_IWS
- EncoderPro
- ePayslip
- Epic
- e-Premis
- Esp
- ESP+Desktop
- ESS
- Essbase Application Manager
- Essbase Excel Add-in
- FAS
- Faxsvr
- FeedbackMonitor
- FISH
- FMRReport
- FormFast
- Formengine
- FRx Designer
- FRx Report
- FusionServer
- Fwpolicy
- GeBIZ
- GEHA
- Global Request System
- GM Supply Power
- Gmail
- GoldMine
- GotoCMC
- Great-West
- Hb.sfcu.org
- HBOWEM (Star)
- Health Fusion
- Health Net
- HealthcareEducation
- HealthStream
- HealthStream-Admin
- HLV
- HMS
- Homecare
- Horizon Meds Manager
- (HMM)
- HRS-D
- Hyperion Planning
- Hyperion Reports
- Ibex
- IBM\_personal\_communications
- icChart
- IEConnect
- IEI
- IEX
- iheatclient
- iHR
- IMaCS
- ImageCast
- Intellisync
- iPharm
- IRSS Web
- iSeries
- iSite\_radiology
- iTelecash
- iTelecash
- JCRACcreditation
- Jre
- Keppel Webmail
- Kinwin32
- Kml
- Kronos
- KronosWeb
- Lab Monitor
- LabTracker
- Lastword
- Launch32
- Learn
- Learn iT
- Legal Billing System
- Loginw32
- Lotus Notes
- Lotus Notes - Ver 6
- LRTS
- MagicWeb
- Mainframe Application
- MaterialsMgmt
- MAX
- McKesson Care Manager
- Mckesson Star
- MckessonSupply
- Md2001
- Mdiapp
- Medgician
- Medi-Cal
- Meditech
- Meditech Web
- MedSeries4
- MISIP
- Misys
- Mp2
- Mplus-Patient-Lookup
- MRMS
- MRS
- MS Access Database
- MS4 Data Transfer
- MS4 Data Transfer Excel
- MSN Messenger
- Muse CV
- Novell Client
- Novius
- Ntracts
- Obix
- oexplore
- OneStaff
- Oracle Financials
- Outlook
- Outlook Express
- Outlook Web Access
- PacifiCare
- PACS
- Pacwin
- Passport
- Pathways Reports
- Pcsws
- PensionExpress
- PeopleSoft
- PeopleSoft Financials
- PeopleSoft HR
- PFM
- PGP
- PHS
- Physician Portal
- PMM
- PMPA
- Pom
- Powerscribe
- PrecyseEdit
- PrecyseNet
- PrivilegeInquiry
- PROCOMM PLUS Workplace
- Putty
- QCI
- Quadramed
- Quality Edge
- Quantim
- Quantros
- Radiology Monitor
- RAS
- RCA
- RedDot
- ReDoc Application
- Reflection
- Reflection
- REG
- Remedy
- Remote Desktop Client
- ReportXpress
- RiskMonitor
- RMReport
- RR5
- Rumba
- RunAs
- Santa Clara IPA
- SAP
- SAP - Ver 6
- SAP Enterprise Portal
- Schwab.com
- SecureCRT
- SERS
- Siebel CRM OnDemand
- Skype
- SmarTerm
- SMS Invision
- Soarian\_Clinicals
- Soarian\_Scheduling
- Socrates
- Socrates Proxy Authentication
- SoftLab
- SoftMed
- SOS
- Spacelabs - ICS
- Sqaman32
- Sr\_gui
- Ssadmin
- Ssexp
- Staffware Process Client
- StaplesLink
- STAR
- Stentor
- Stix
- T4\_Scheduling
- TDWeb
- TimePC
- Stentor
- Stix
- T4\_Scheduling
- TDWeb
- TimePC
- TraceMasterVue
- Track-It
- Trendcare
- Trendstar
- TTPLS
- TullyWihr
- United Healthcare Online
- UPS
- VES
- VI\_Client
- Visual DX
- VNC
- VNC Viewer
- VoiceWave
- VolunteerWorks
- WebConnect
- WebMD
- WebMedicityProAccess
- WIINGS
- Windows Logon
- Winnetuse
- WinSCP
- Winspool
- Winspool400
- WS Comets
- Yahoo Messenger
- Yahoo web

Applications

## Fonctionnalité de provisioning utilisateur

- Les fonctionnalités de provisioning sont embarquées dans la solution
- Possibilité d'enrichir directement le coffre-fort personnel
- Support de la gamme
  - Tivoli Identity Manager
- Impact client
  - Une solution IAM intégrée
  - Simplification de la gestion des comptes
  - L'utilisateur final ne doit connaître qu'un seul mot de passe
  - Premier pas de la mise en œuvre d'une politique d'IAM



## Points forts

- Architecture client-server :
  - ▶ Support de la haute disponibilité, pas de surcharge du référentiel existant
  - ▶ Pas de modification de schéma du référentiel client
  
- Pas de modification de la GINA windows, mais un remplacement
  - ▶ Une seule GINA pour tous les modules (kiosk, dpra, authentification)
  - ▶ Toujours possibilité de se logger sur la gina windows, voire de ne pas utiliser la gina Tivoli
  
- Intégration avec + de 300 applications
  
- Module AccessStudio pour construire les modèles simple et intuitive (drag&drop)
  
- Auto-apprentissage simplifié (POST login, un seul clic à faire)
  
- Console d'administration en client léger
  
- Intégration avec TIM
  
- Fonctions de workflows (automatisation dans le lancement d'applications, single sign-off, politiques, etc..)



**Best Identity Management Solution**  
**Best Single Sign-On Solution**  
**Best Second- and Multi-Factor Solution**







## Démonstration



**Questions ?**

**[charles.tostain@fr.ibm.com](mailto:charles.tostain@fr.ibm.com)**