IBM

Charles Tostain

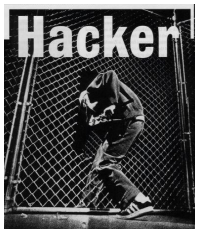
Single Sign-On Tivoli software

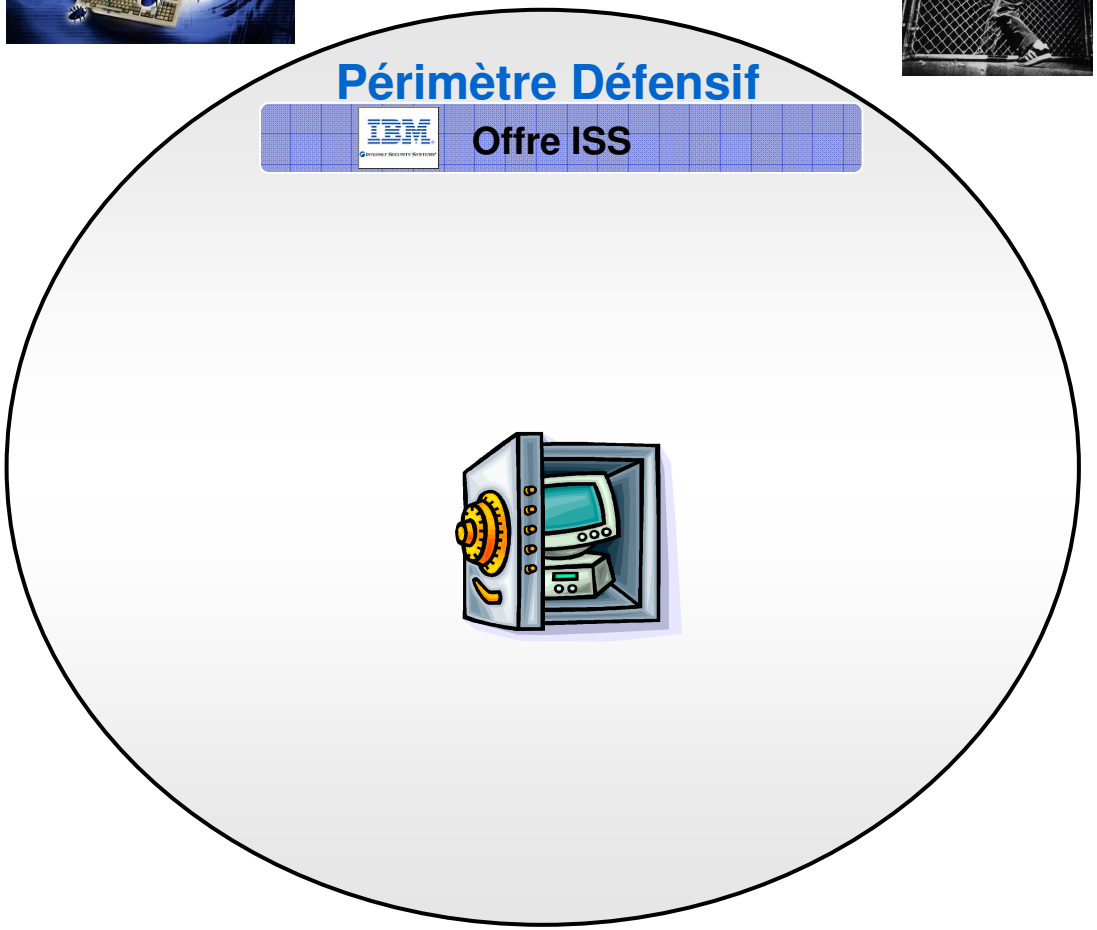
Simplifiez la vie de vos utilisateurs avec le SSO

TENDANCES LOGICIELLES D'ÉTÉ 2008

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

IBM et Tivoli : Les enjeux de la sécurité informatique





Périmètre défensif

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 personne 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.

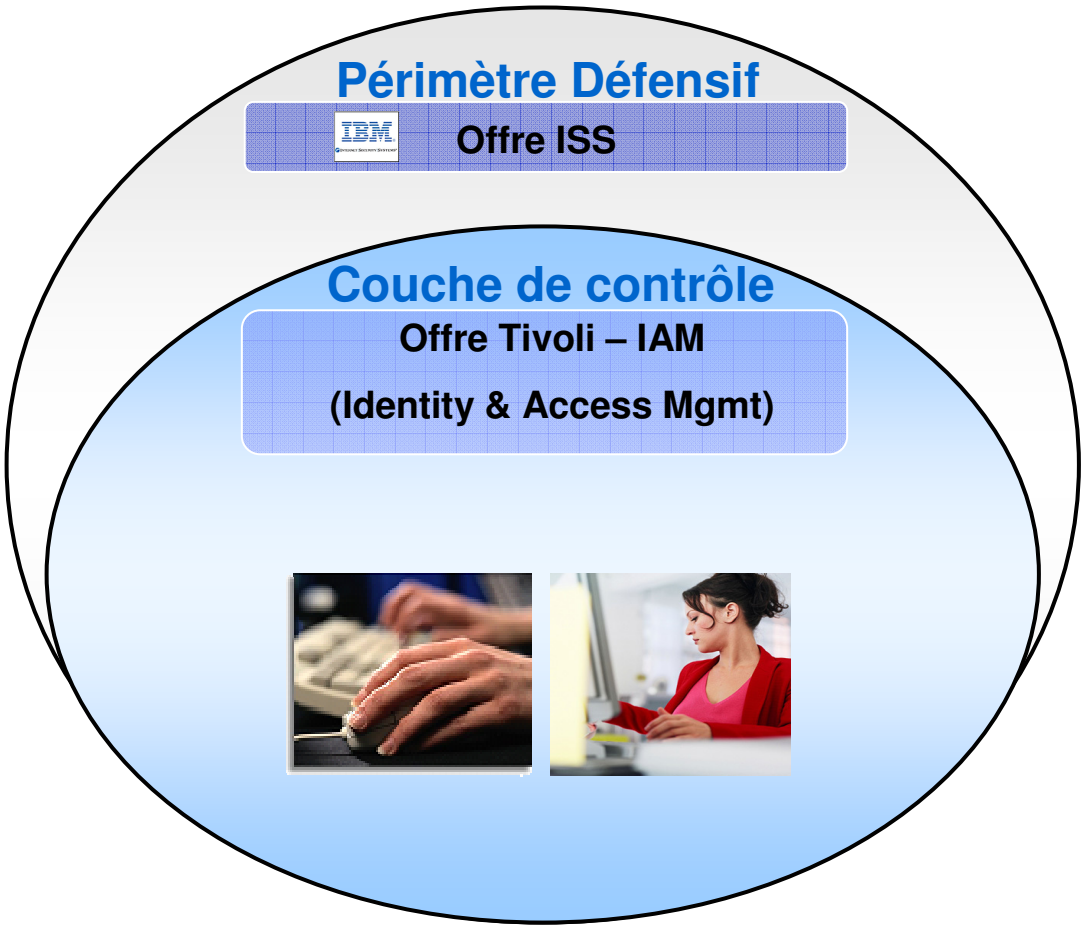
By Larry Greenemeier
InformationWeek
février 15, 2007 03:00 PM

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.

IBM et Tivoli : les enjeux de la sécurité informatique



Périmètre défensif

Fermer la porte aux intrus avec:

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

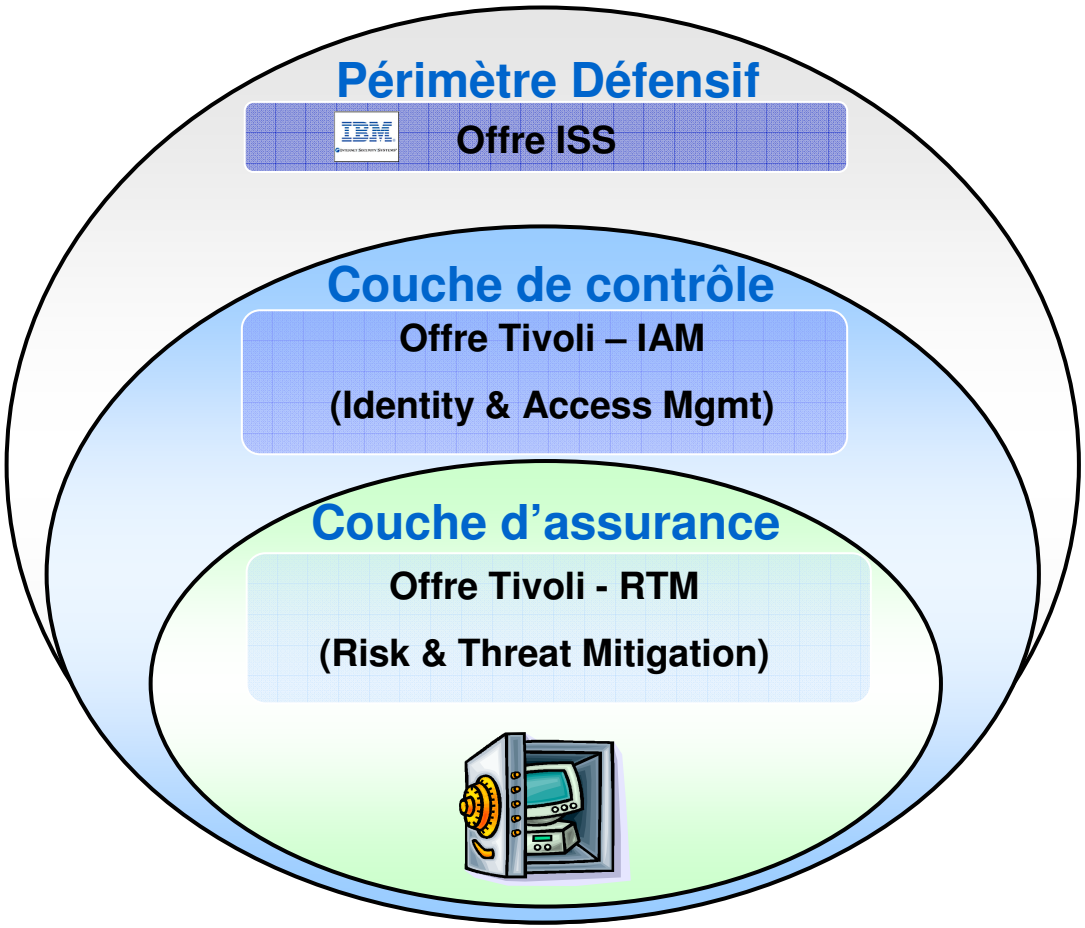
Couche de contrôle

- 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



Périmètre défensif

Fermer la porte aux intrus avec:

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

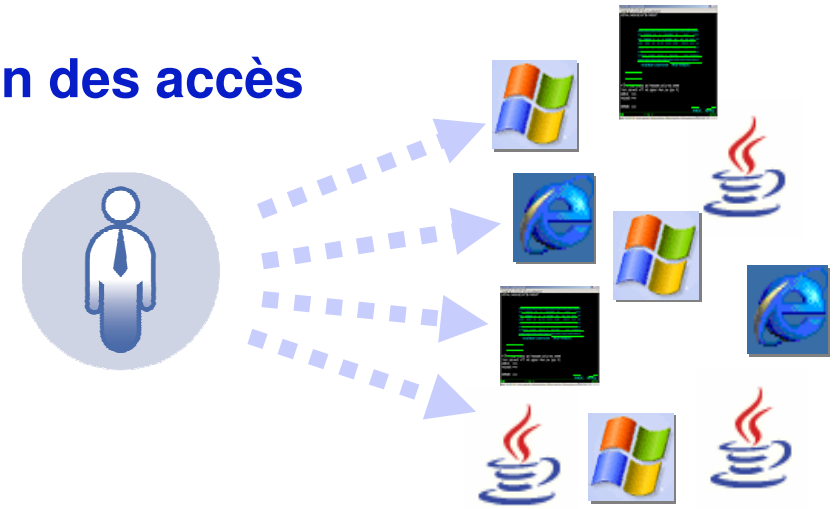
Couche de contrôle

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

Couche d'assurance

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

IAM: Quelques constats
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**

IBM

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

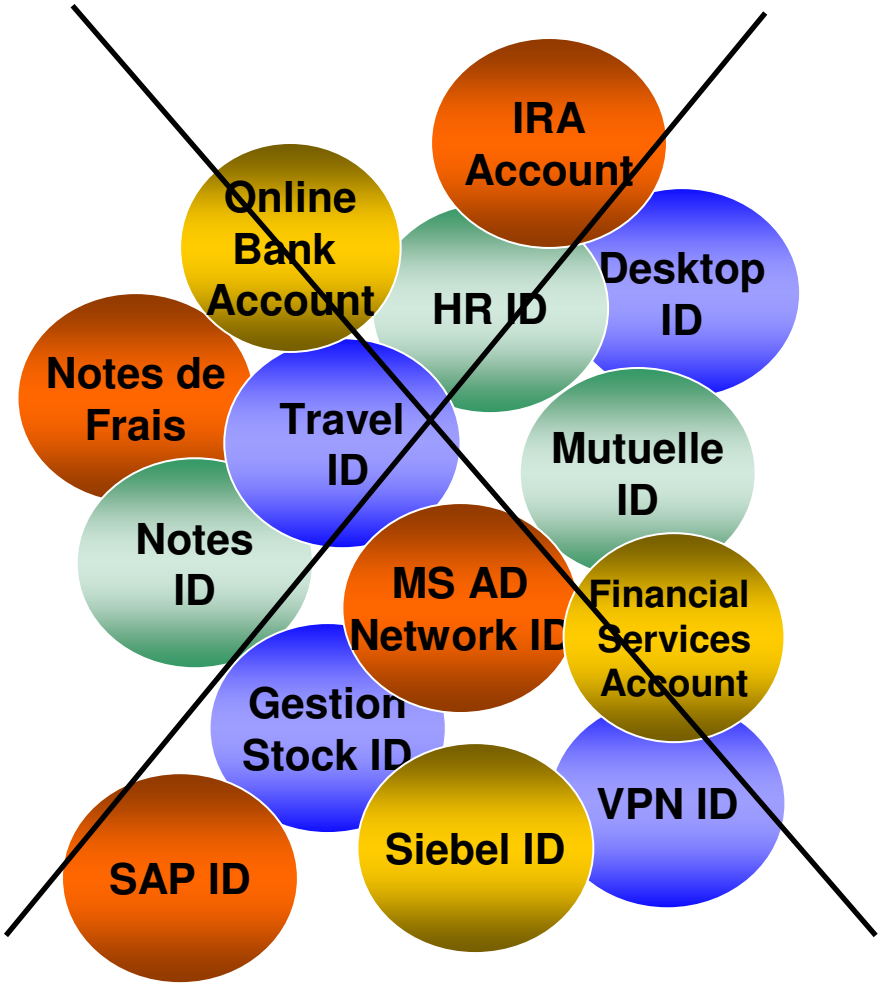
- Nécessité de respecter les nouvelles règlementations
- Les mots de passe doivent être difficiles à pirater

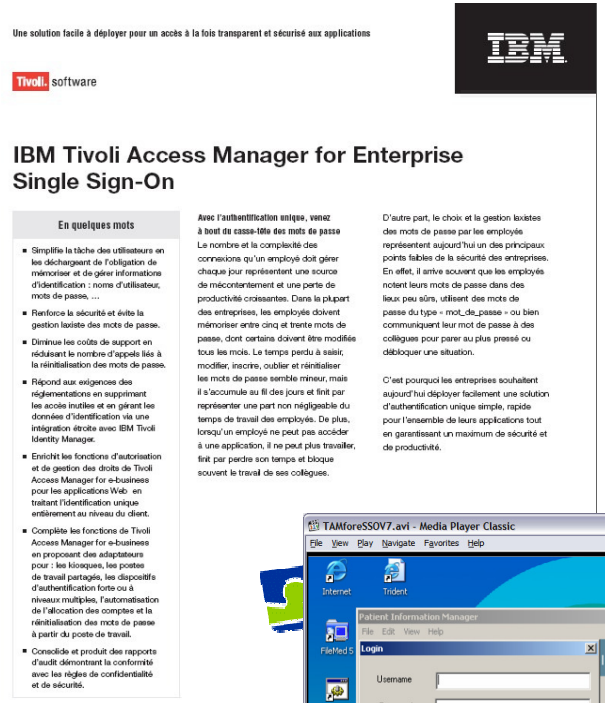
Mots de passe complexes
Qui doivent être changés fréquemment

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.

L'authentification unique
Un moyen rapide pour impliquer les utilisateurs





Une solution facile à déployer pour un accès à la fois transparent et sécurisé aux applications

Tivoli. software

IBM

IBM Tivoli Access Manager for Enterprise Single Sign-On

En quelques mots

- Simplifie la tâche des utilisateurs en les déchargeant de l'obligation de mémoriser et de gérer informations d'identification : noms d'utilisateur, mots de passe, ...
- Renforce la sécurité et évite la gestion laxiste des mots de passe.
- Diminue les coûts de support en réduisant le nombre d'appels liés à la réinitialisation des mots de passe.
- Répond aux exigences des réglementations en supprimant les accès inutiles et en gérant les données d'identification via une intégration étroite avec IBM Tivoli Identity Manager.
- Enrichit les fonctions d'autorisation et de gestion des droits de Tivoli Access Manager for e-business pour les applications Web en traitant l'identification unique entièrement au niveau du client.
- Complète les fonctions de Tivoli Access Manager for e-business en proposant des adaptateurs pour : les kiosques, les postes de travail partagés, les dispositifs d'authentification forte ou à niveaux multiples, l'automatisation de l'allocation des comptes et la réinitialisation des mots de passe à partir du poste de travail.
- Consolide et produit des rapports d'audit démontrant la conformité avec les règles de confidentialité et de sécurité.

Avec l'authentification unique, venez à bout du casse-tête des mots de passe

Le nombre et la complexité des connexions qu'un employé doit gérer chaque jour représentent une source de mécontentement et une perte de productivité croissantes. Dans la plupart des entreprises, les employés doivent mémoriser entre cinq et trente mots de passe, dont certains doivent être modifiés tous les mois. Le temps perdu à saisir, modifier, inscrire, oublier et réinitialiser les mots de passe semble mineur, mais il s'accumule au fil des jours et finit par représenter une part non négligeable du temps de travail des employés. De plus, lorsqu'un employé ne peut pas accéder à une application, il ne peut plus travailler, finit par perdre son temps et bloque souvent le travail de ses collègues.

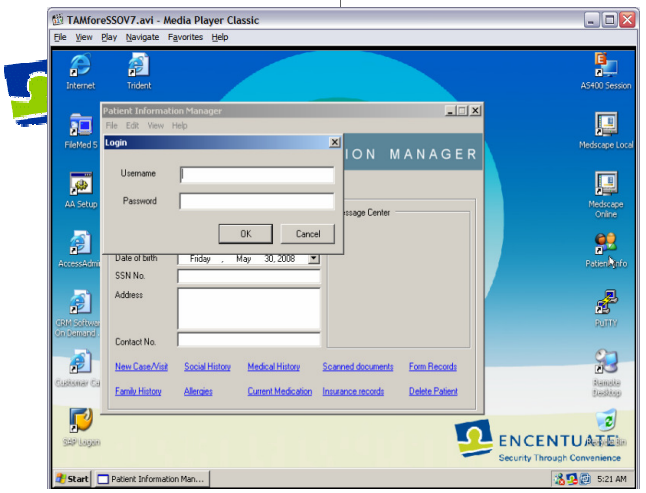
D'autre part, le choix et la gestion laxistes des mots de passe par les employés représentent aujourd'hui un des principaux points faibles de la sécurité des entreprises. En effet, il arrive souvent que les employés notent leurs mots de passe dans des lieux peu sûrs, utilisent des mots de passe du type « mot_de_passe » ou bien communiquent leur mot de passe à des collègues pour parer au plus pressé ou débloquer une situation.

C'est pourquoi les entreprises souhaitent aujourd'hui déployer facilement une solution d'authentification unique simple, rapide pour l'ensemble de leurs applications tout en garantissant un maximum de sécurité et de productivité.

Pratiquement aucune ressource d'administration nécessaire

Simple, rapide à déployer, ROI immédiat

Conçu pour les utilisateurs

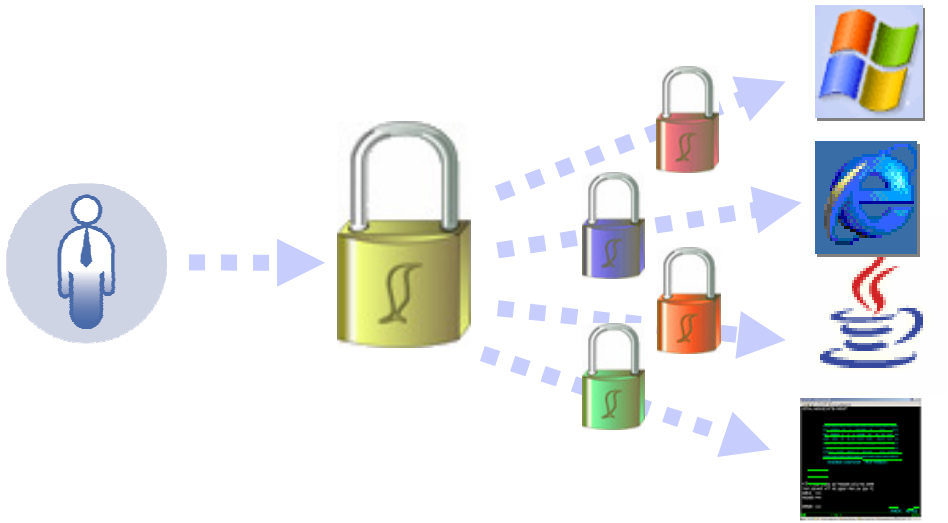


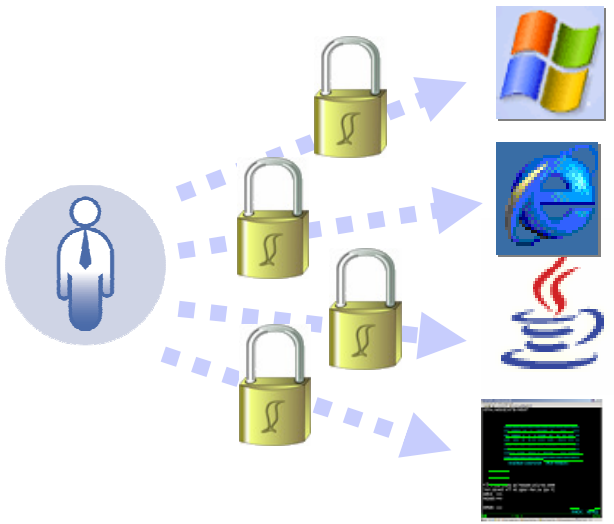
SSO Entreprise ou Poste de Travail : SSO étendu

- 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

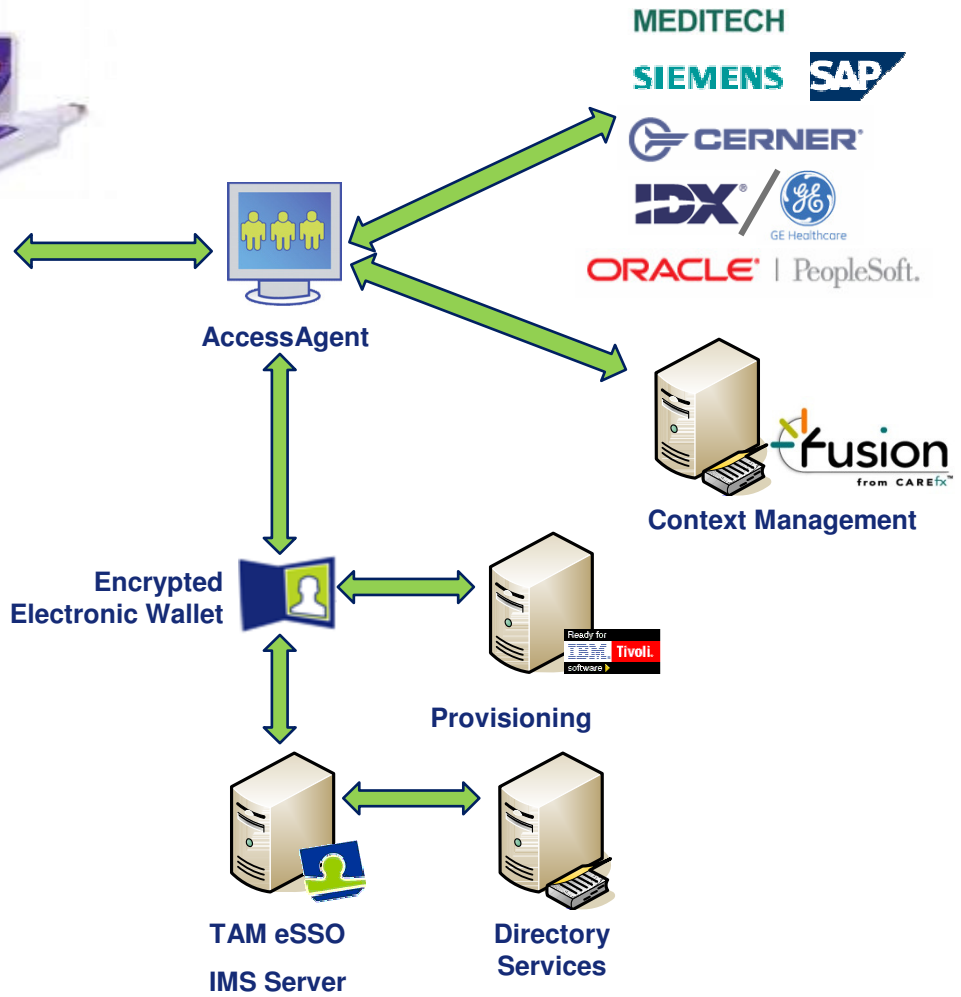
A ne pas confondre !

SIGNATURE UNIQUE (SSO) ≠ MOT DE PASSE UNIQUE (Synchro)





TAM for eSSO

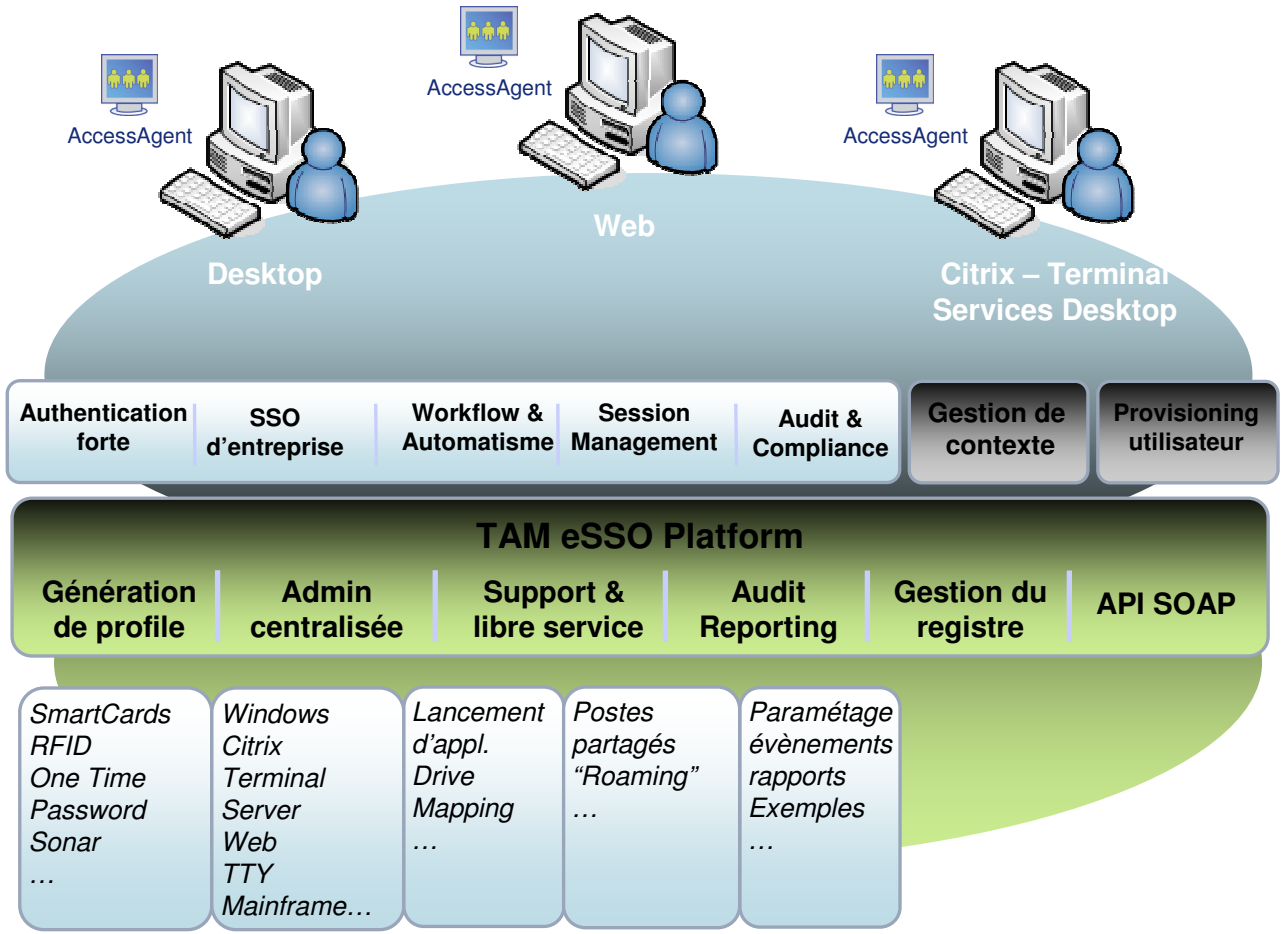


- ESSO, Automatisation et Workflow & Gestion du contexte utilisateur
- Two-Factor Authentication & Traçabilité des accès
- Login rapide & Accès à tout type d'application
- Identité centralisée & Gestion des polices & Audit
- Ne requiert aucune modifications
- Gestion de la conformité

Un support étendu du SSO pour tout type de terminaux

TAM eSSO:

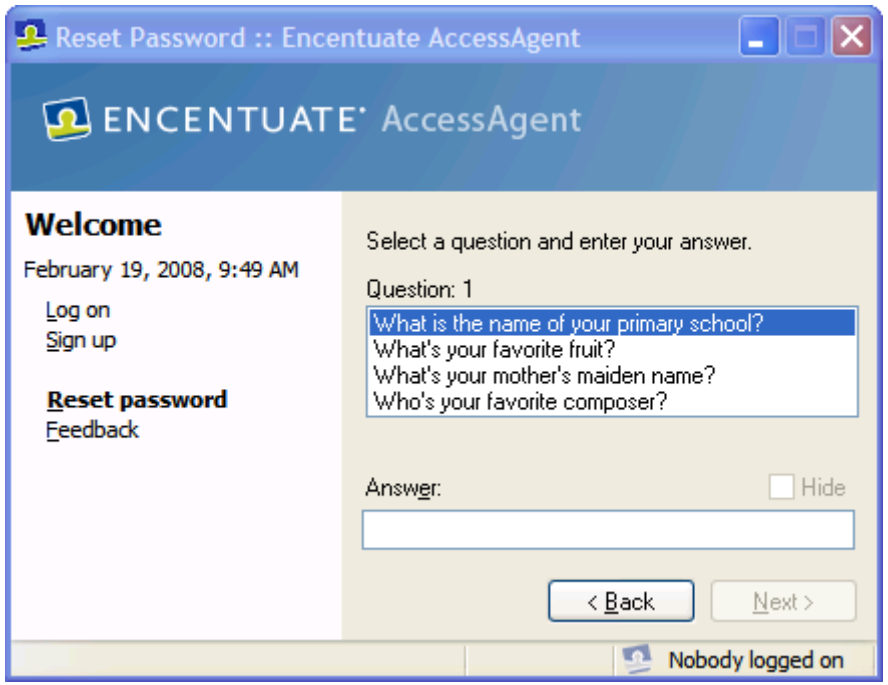
- Simplifie l'expérience utilisateur et améliore la productivité en éliminant le besoin de se souvenir de multiple identité et mot de passe
- Facilite la mise en oeuvre de la compliance avec les fonctionnalités de traçabilité et en collectant les accès
- Améliore la sécurité en éliminant les mot de passe 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*

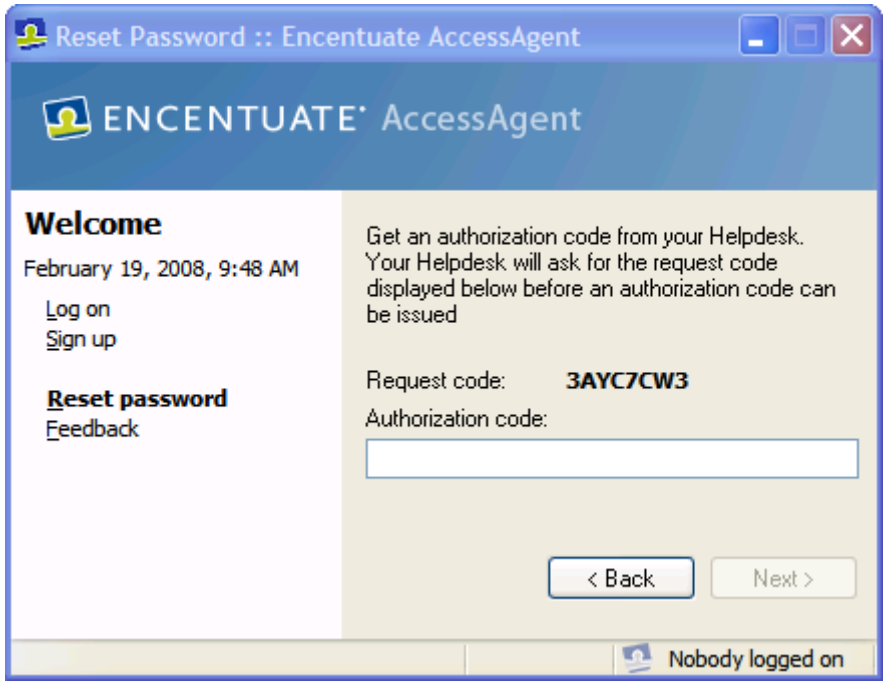
Autres fonctions: Self-service Reset

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



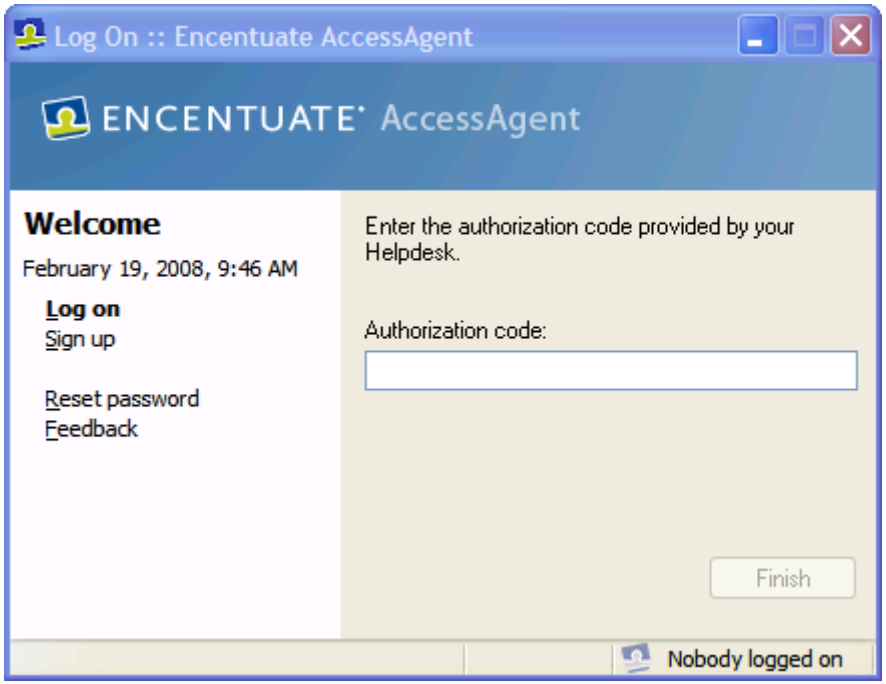
Autres fonctions: Reset offline

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

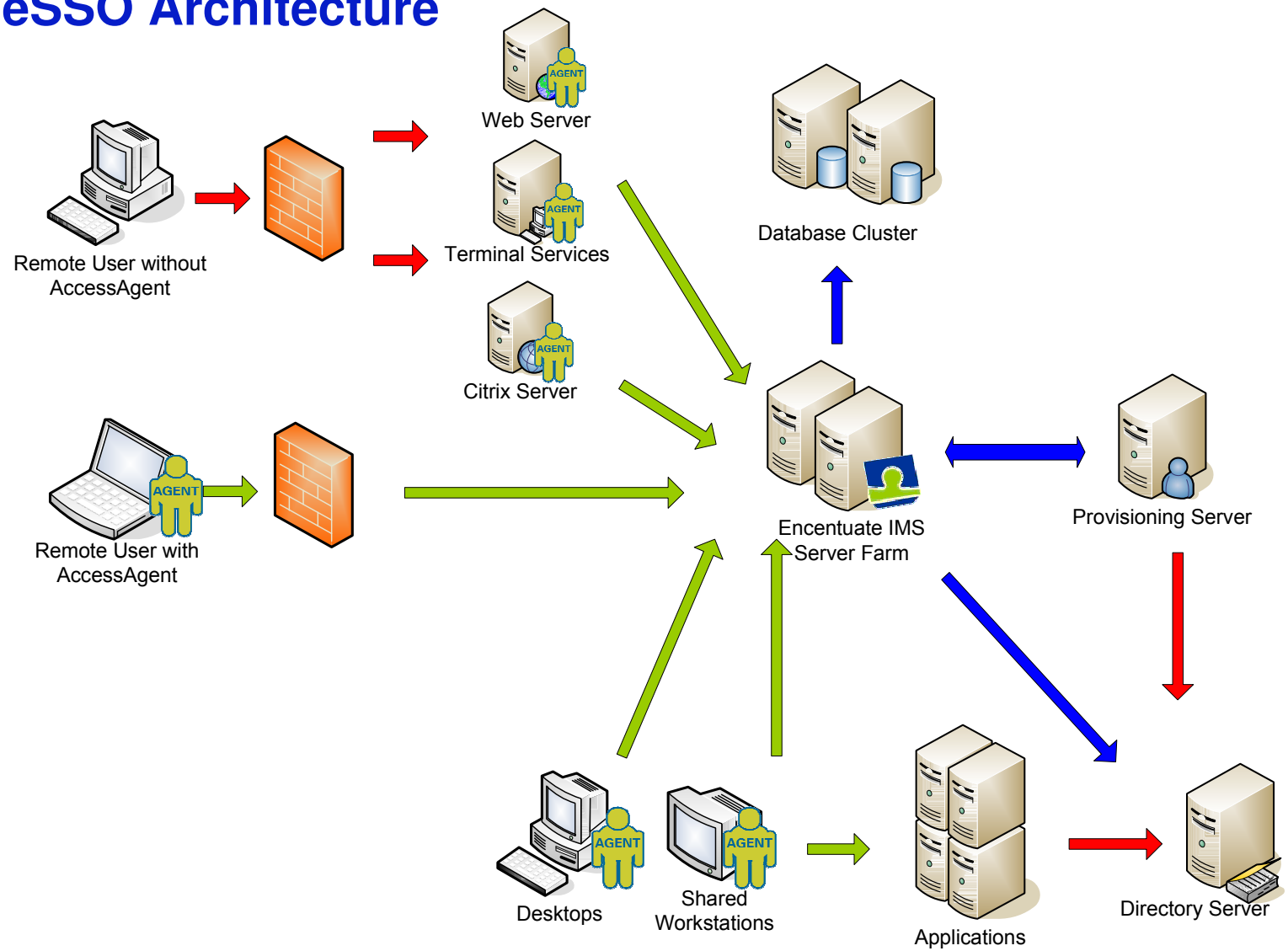


Autres fonctions: Cas de perte de l'authentification forte

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



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
Calllog32
CapitalAdvisor
Captura
Careman
CareManager
CBISA-WebEntry
Centicity RIS Technologist
Centricity RIS Equipment Manager
Centricity RIS Key Word Search
Centricity RIS
Mammography Tracking
Centricity RIS Order Management
Centricity RIS Radiology
Centricity RIS Repotr 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
Computrition
Connect32
Content Manager
Cplgv
CPRS
Cprtm
Cpsecuremotepw
CPSS Enquiry
CPSS Production
Cpstat
Cpusermonitor
Craneware
CRM
CWEB
DBS.com
DCHS Access
Dchsnet
DDE
Designer
DSG Support
DSG-GUI
Eaadmin32
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
Faxsrvr
FeedbackMonitor
FISH
FMReport
FormFast
Formsengine
FRx Designer
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
MISP
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
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
TENDANCES LOGICIELLES IT&E 2006
SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

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 logguer 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, policies, etc..)

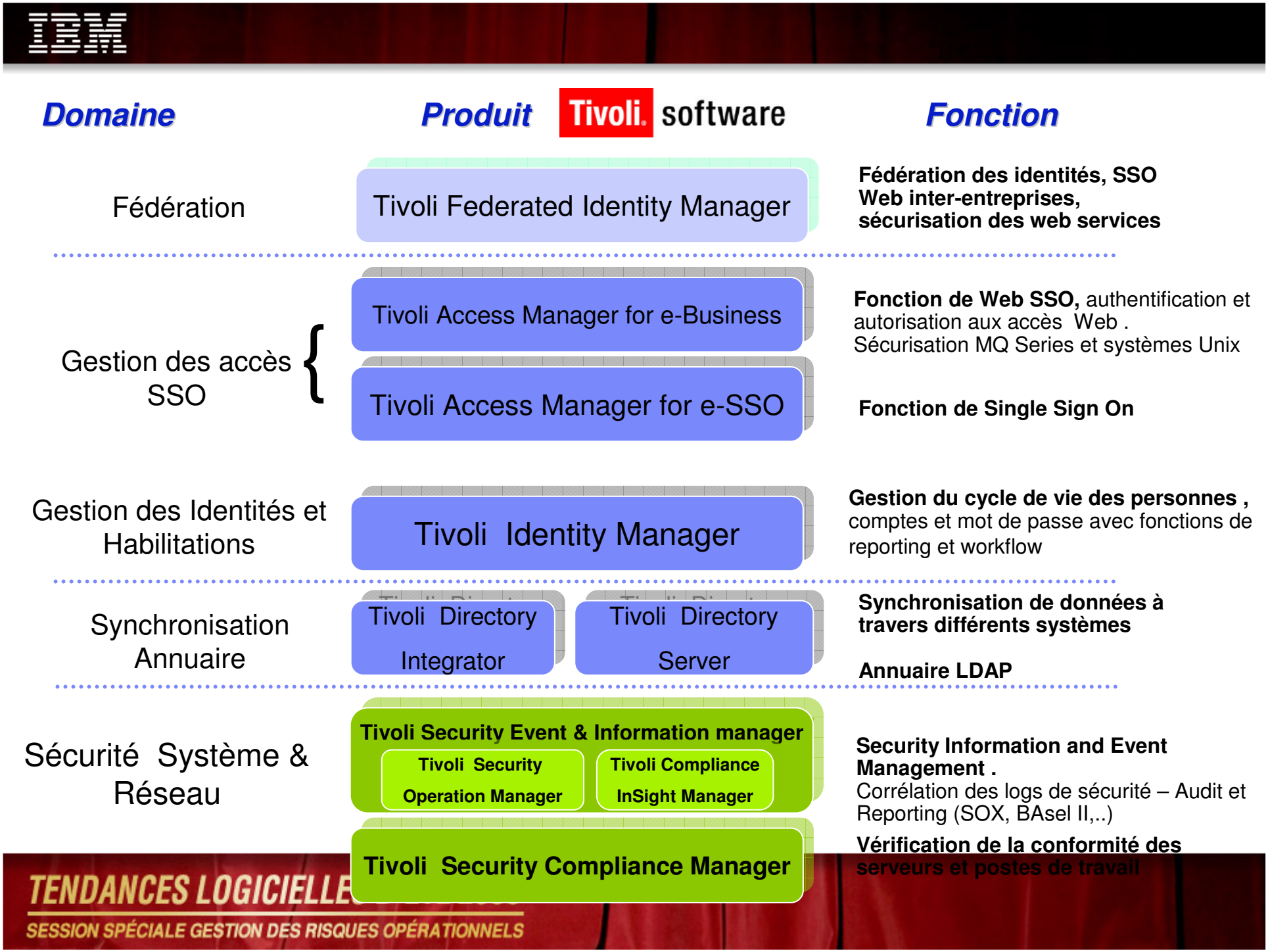
Les bénéfices de Tivoli Access Mgr for Enterprise Single Sign-on

- Simplifie l'expérience utilisateur en éliminant la nécessité de se souvenir de tous ses mots de passe
- Améliore la sécurité en renforçant la complexité des mots de passe et en éliminant les risques liés à l'utilisateur…
- Réduction des coûts du help desk (baisse des appels pour reset de mot de passe)
- Déploiement sans modification sur les systèmes cible: retour sur investissement rapide
- Premier pas vers la gestion des identités, la conformité et l'intégration de solutions d'authentification…

Questions ?

charles.tostain@fr.ibm.com

Backup slides


Domaine
Produit
Tivoli software
Fonction
Fédération
Tivoli Federated Identity Manager
Fédération des identités, SSO Web inter-entreprises, sécurisation des web services
Gestion des accès SSO
Tivoli Access Manager for e-Business
Fonction de Web SSO, authentification et autorisation aux accès Web . Sécurisation MQ Series et systèmes Unix
Tivoli Access Manager for e-SSO
Fonction de Single Sign On
Gestion des Identités et Habilitations
Tivoli Identity Manager
Gestion du cycle de vie des personnes , comptes et mot de passe avec fonctions de reporting et workflow
Synchronisation Annuaire
Tivoli Directory Integrator
Tivoli Directory Server
Synchronisation de données à travers différents systèmes
Annuaire LDAP
Sécurité Système & Réseau
Tivoli Security Event & Information manager
Tivoli Security Operation Manager
Tivoli Compliance InSight Manager
Security Information and Event Management . Corrélation des logs de sécurité – Audit et Reporting (SOX, BAsel II,..)
Tivoli Security Compliance Manager
Vérification de la conformité des serveurs et postes de travail
TENDANCES LOGICIELLE
SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

Plans for IBM Tivoli Access Manager for Enterprise Single Sign-on Packaging and Pricing

Standard License

- Core ESSO functionality
- Self-service password reset
- Centralized logging
- $69 per user

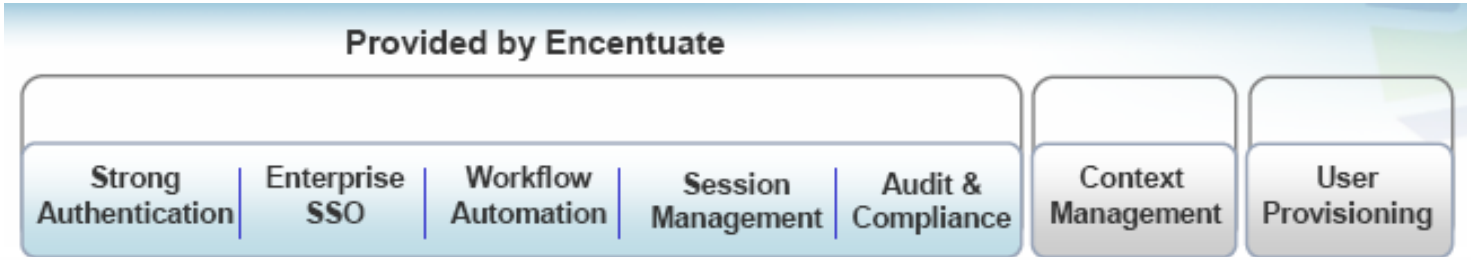
Suite License

- Standard license plus…
- Strong authentication and user provisioning support
- Session management and workflow automation
- Customized tracking
- $99 per user

QuickStart Services

- 500 user license, 1 year support, 10 days of services, limited set of applications
- Standard QuickStart $35k, Suite QuickStart $50k
- Availability TBD – based on skill ramp up

Encentuate SSO Suite



Strong authentication
- Building badge integration
- Active RFID
- Fingerprint biometric
- USB Smart Cards
- Cell phone authentication
- OTP

ESSO
- For Win/Citrix/TS/thin client platforms
- For Web/Desktop and Mainframe/TTY apps
- Browser-based SSO
- Auto-generation of SSO AccessProfiles

Workflow Automation
- Application launch, drive mapping, user switching, single sign-off, etc
- Walk-away desktop security

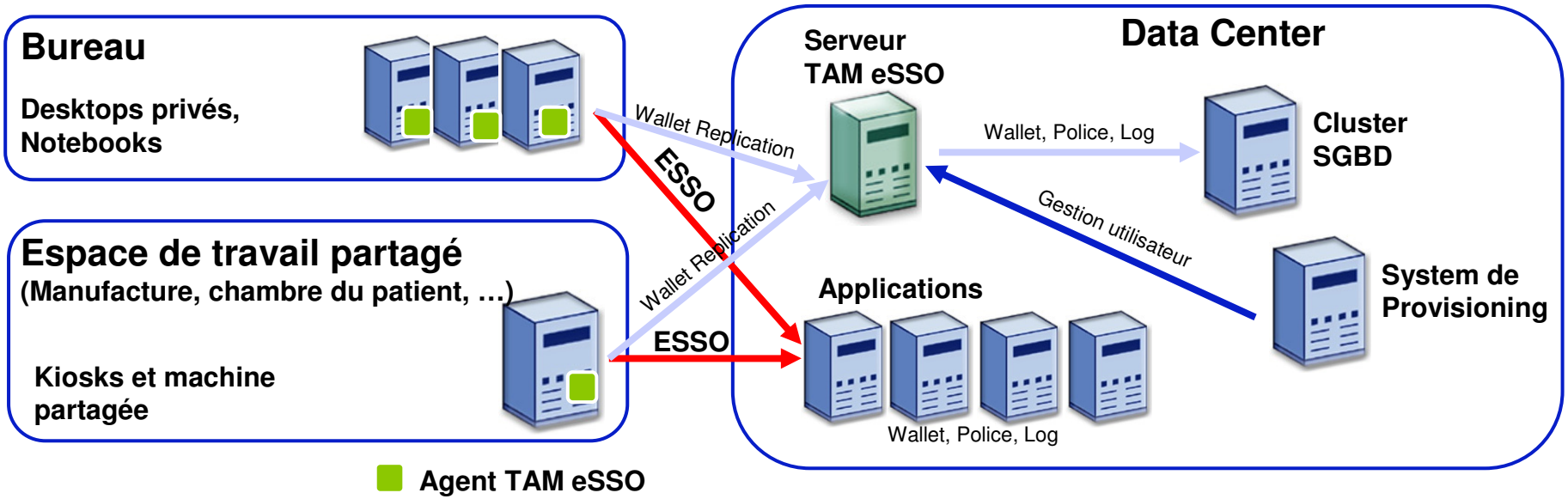
Session Management
- Shared Desktops
- Roaming Desktops
- Private Desktops

Centralized Admin
- Web-based AccessAdmin
- Group-based, policy-driven mgmt

Support and Self-Service
- Loss management
- User Self-service

Centralized Audit
- End-point tracking
- Centralized SQL reporting

Les capacités de la solution TAM eSSO



Capacités de TAM eSSO

Enterprise Single Sign-on
- Automatise le sign-on des applications web, Java et Mainframe (plus de 300 en standard)

Gestion de la session
- Fonction de transition d'utilisateur sur des environnement partagés (Shared ou roaming desktops)
- Conserve les applications, données et connections

Bureau (Desktop/Notebook)
- La réplication en local permet le mode déconnecté

Support des méthodes d'identification
- Identité & mot de passe
- One time passwords, USB tokens
- Smart cards, RFID, lecteur de badge et carte
- Biometrique

Espace partagé
- La gestion de multiple identité en local permet à différents utilisateurs de partager le même espace de travail et la fonction de SSO (e.g. workstation in ER of hospital)

Audit et rapport
- Logger, collecter, alerter et reporter les accès aux données fait par les utilisateurs en vue de la mise en œuvre de la conformité