Gestion de l'Identité

Jean-Paul Bembaron

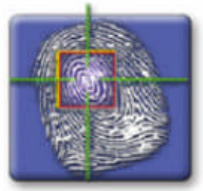
Sun Microsystems France

Java

Sun microsystems
We make the net work.

Les fonctions d'identités (lexique)

Identification - Qui je suis ?



Authentification - Je prouve qui je suis

Habilitation - Quels sont mes droits ?

La gestion de l'identité ?

- Implémentation des processus entreprise de gestion des utilisateurs
  - Workflow
  - Scénario
- Tâches d'administration courantes
  - Création de comptes dans les applications du SI
  - Gestion du cycle de vie des identités (utilisateurs) :
    - Ajout, modification, suppression, activation,désactivation, déverrouillage
    - Gestion du mot de passe
    - Création de profils, affectation de profils
- Délégation de l'administration
  - Modèle de délégation ouvert, auto-administration
- Outils de contrôle
  - Audit
  - Gestion de risque

Gestion de l'Identité

Jean-Yves Pronier

Sun Microsystems France

Java

Sun microsystems

We make the net work.

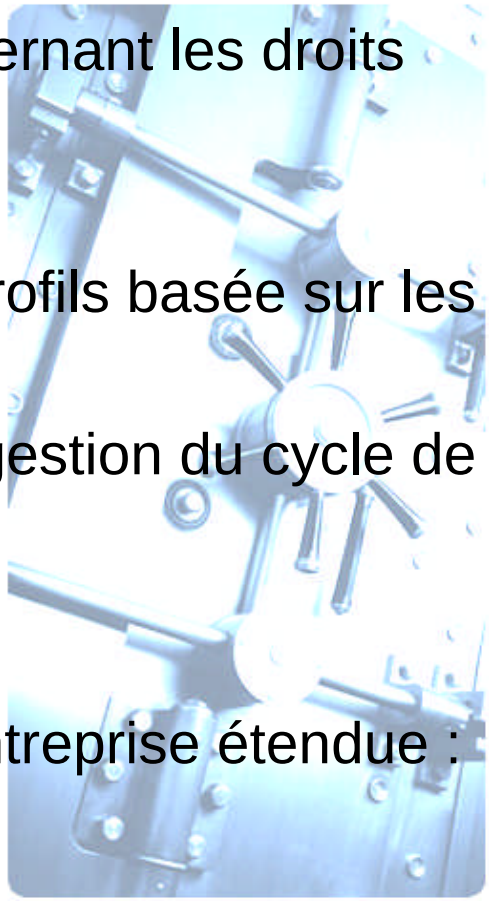
Quels Enjeux et quels bénéfices ?

- 3 domaines impactés :
  - La Sécurité
  - La Productivité
  - La Mise en Conformité

Quels Enjeux et quels bénéfices ?

La Sécurité :

- Renforcement de la politique de sécurité concernant les droits d'accès au système d'information :
  - Gestion temps-réel des comptes orphelins
  - Gestion permanente des autorisations et profils basée sur les rôles des utilisateurs
- Point de contrôle unique et centralisé pour la gestion du cycle de vie des utilisateurs du SI
- Automatisation des tâches d'administration
- Elargissement de la politique de sécurité à l'entreprise étendue :
  - Fournisseurs, Partenaires et Clients



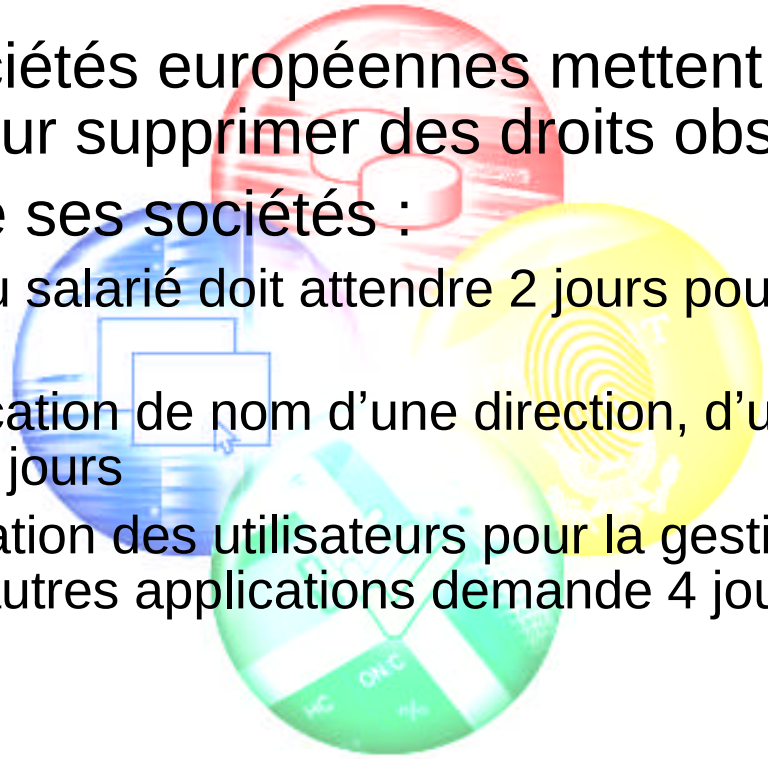
Quels Enjeux et quels bénéfices ?

La Productivité :

- Confort et productivité des utilisateurs :
  - Maintenance et auto-administration des “passwords” et profils
- Allègement des ressources de ”hot line” ou de “call center”
  - Réduction de 30% en moyenne
- Meilleurs niveaux de services :
  - Intégration des solutions à l'ensemble du patrimoine applicatif
  - Propagation automatique des informations (droits & profils)
- Audits et Reporting automatisés :
  - Permanents et temps-réels

Assurer la mise en conformité

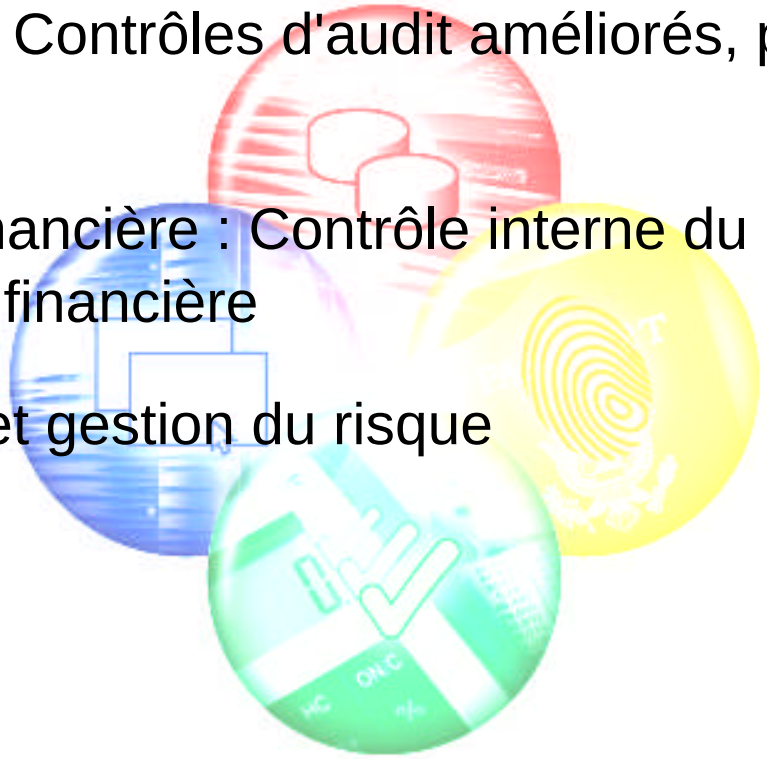
- État des lieux à titre d'exemple et dans le meilleur des cas :
  - 20% des sociétés européennes mettent plus de 2 semaines pour supprimer des droits obsolètes
  - Pour 48% de ses sociétés :
    - Un nouveau salarié doit attendre 2 jours pour obtenir ses codes d'accès
    - Une modification de nom d'une direction, d'un département nécessite 2 jours
    - L'administration des utilisateurs pour la gestion des processus métiers et autres applications demande 4 jours par mois



Quels Enjeux et quels bénéfices ?

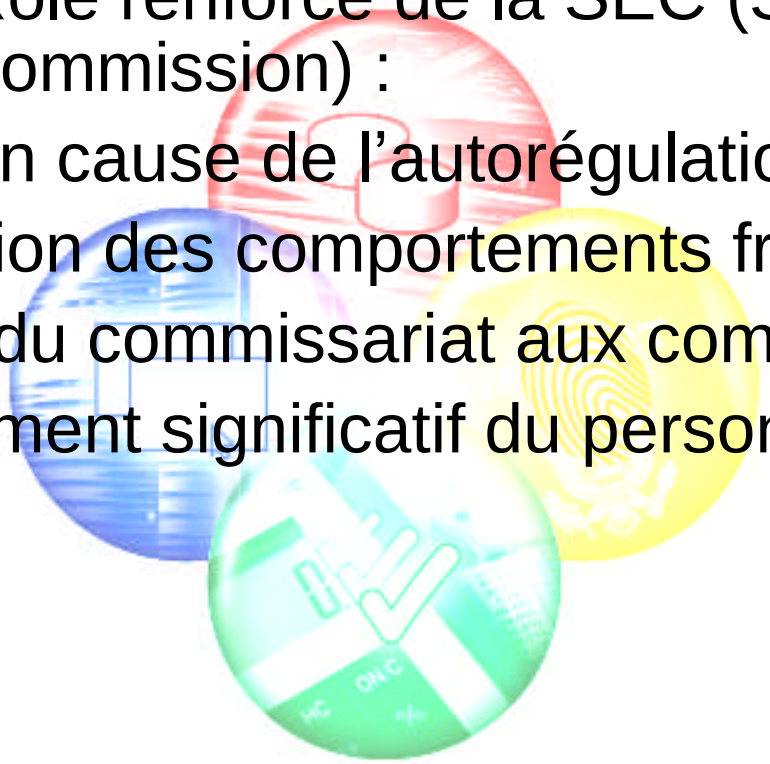
La Mise en Conformité :

- Sarbanes-Oxley – Contrôles d'audit améliorés, protection des investisseurs
- Loi de sécurité Financière : Contrôle interne du reporting financier et communication financière
- Bale II : Contrôle et gestion du risque



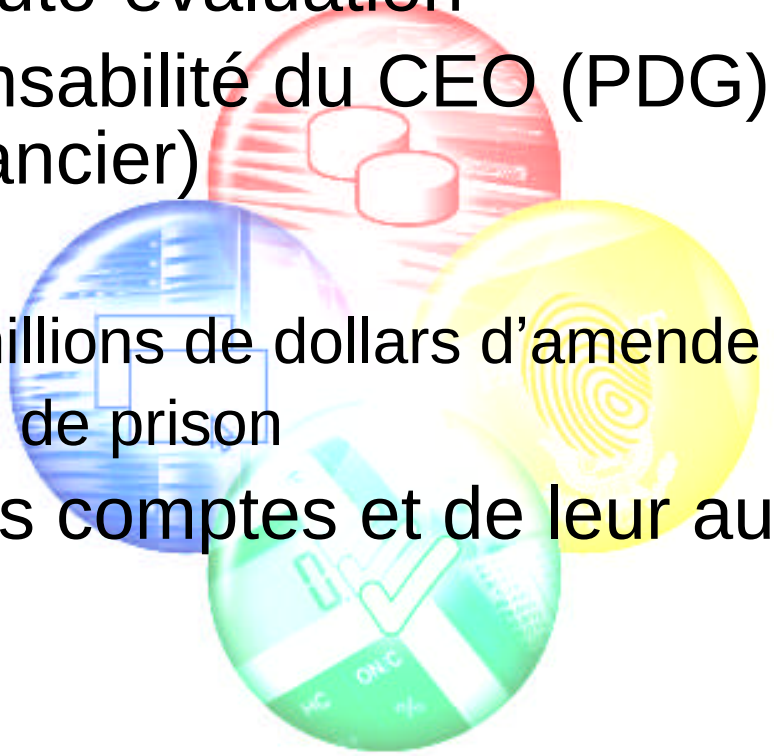
Sarbanes Oxley Act

- Suite à ENRON, WORLDCOM, TYCO…
- Une loi écrite ne fournissant qu'un cadre général
- Finalités – Rôle renforcé de la SEC (Securities and Exchange Commission) :
  - Remise en cause de l'autorégulation
  - Pénalisation des comportements frauduleux
  - Réforme du commissariat aux comptes
  - Renforcement significatif du personnel et du budget



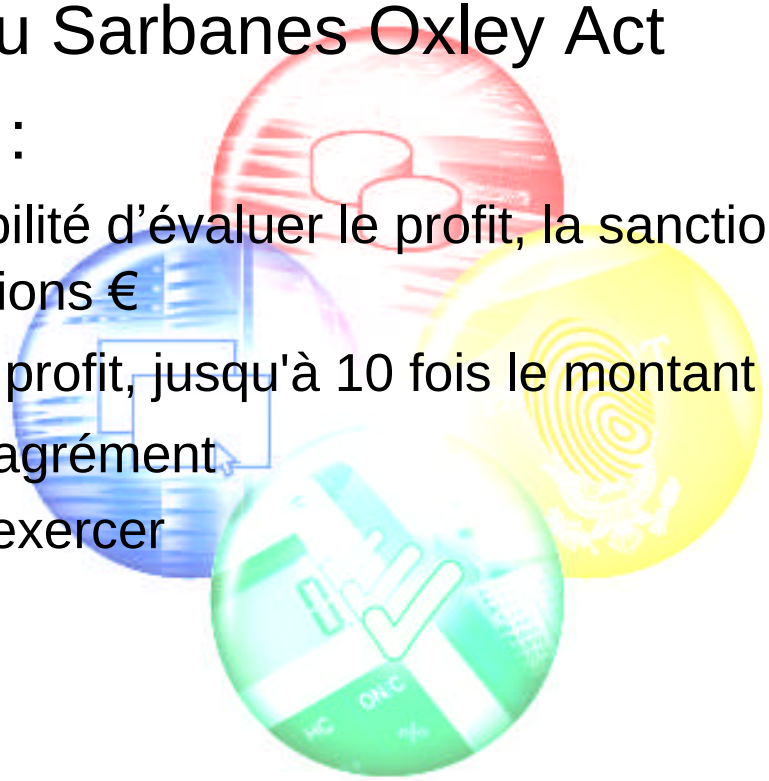
Sarbanes Oxley Act

- Certification des comptes de la société et des rapports périodiques
- Fondée sur l'auto-évaluation
- Sous la responsabilité du CEO (PDG) et du CFO (Directeur Financier)
- Sanctions :
  - De 2,5 à 25 millions de dollars d'amende
  - De 5 à 20 ans de prison
- Importance des comptes et de leur authenticité



Loi de Sécurité Financière

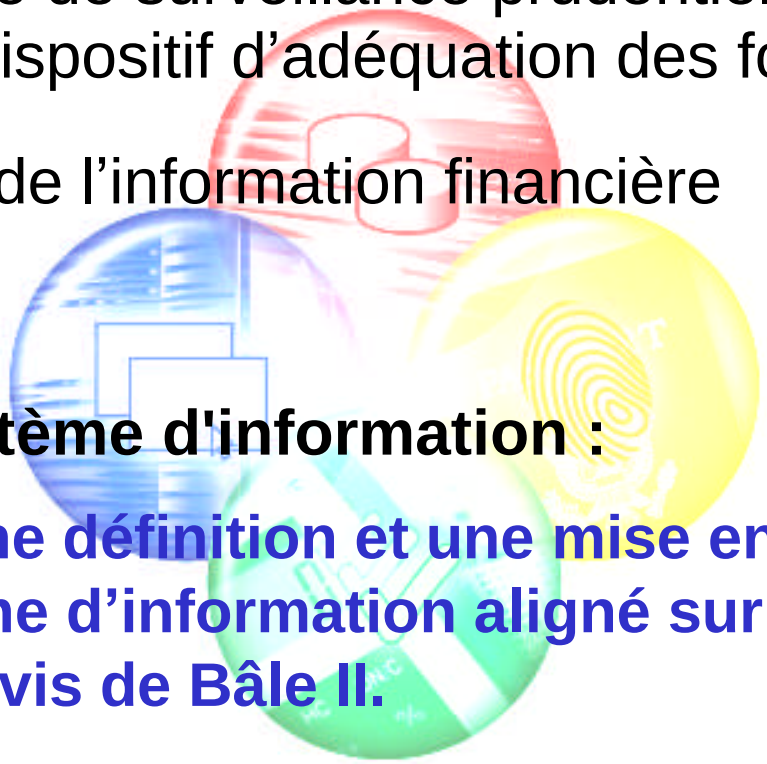
- Suite au Crédit Lyonnais, à Vivendi…
- Imposer la transparence financière
- Dans l'esprit du Sarbanes Oxley Act
- Des sanctions :
  - Dans l'impossibilité d'évaluer le profit, la sanction ne peut aller au delà de 1,5 millions €
  - Dans le cas de profit, jusqu'à 10 fois le montant du profit
  - Suppression d'agrément
  - Impossibilité d'exercer
  - ...



Bale II

Bâle II réglemente trois axes :

- une nouvelle exigence minimale de fonds propres
- une mise en place de surveillance prudentielle renforcée homologuant le dispositif d'adéquation des fonds propres
- un renforcement de l'information financière



Impacts sur le système d'information :

- **Cela entraîne une définition et une mise en œuvre d'un nouveau système d'information aligné sur les besoins bancaires vis-à-vis de Bâle II.**

Les types d'événements caractérisant le Risque Opérationnel :

- la fraude interne : le défaut intentionnel d'information sur les positions, le **vol par un employé et le virement interne sur le compte détenu par un employé**

- la fraude externe : le vol, la contrefaçon, le chèque de cavalerie et les **dommages résultant d'un piratage informatique**

- les clients, les produits et les procédures de gestion : **les transactions interdites sur les comptes de la banque**

- les perturbations des processus métiers et les pannes de système : les pannes de matériel et de logiciel, les problèmes de télécommunication et les pannes issues de services sous-traités

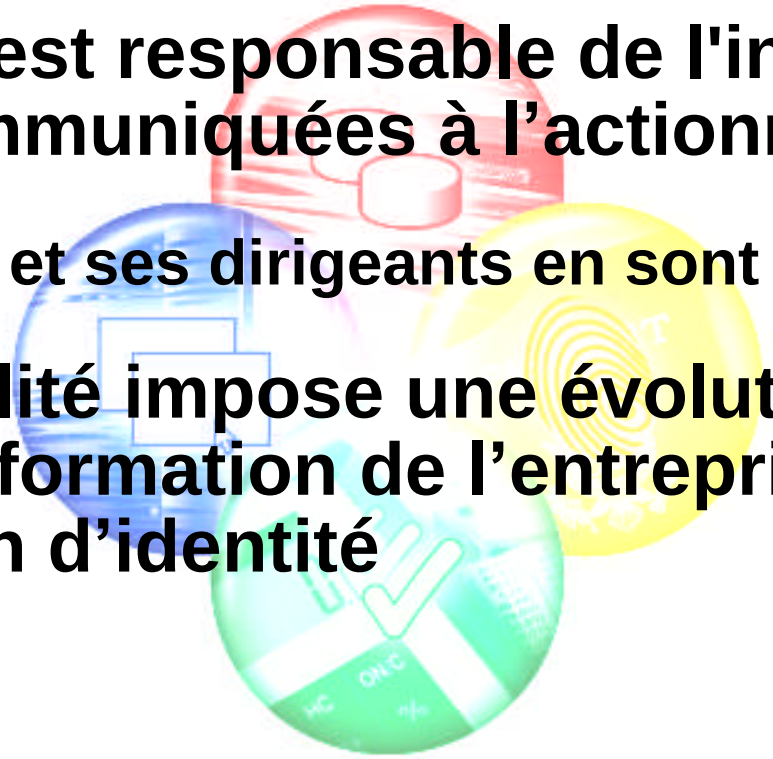
- l'exécution, le résultat et le contrôle de processus : les erreurs de saisie de données. **l'accès non autorisé donné aux comptes de**

Contrôles du système d'information

- Gestion d'identité
  - Authentification unique (SSO)
  - Habilitation (profil, rôle…)
  - Autorisation, droit d'accès, délégation
- Gestion de clé (PKI)
  - Signature
  - Certification
- Sécurisation de la messagerie, des accès à Internet
- Gestion documentaire :
  - Archivage
  - Sauvegarde
  - tiers de confiance

Une première conclusion

- **De la vache folle à Enron, un seul mot la traçabilité**
- **L'entreprise est responsable de l'intégrité des données communiquées à l’actionnaire**
  - **L’entreprise et ses dirigeants en sont responsables**
- **Cette traçabilité impose une évolution du système d’information de l’entreprise reposant sur la gestion d’identité**

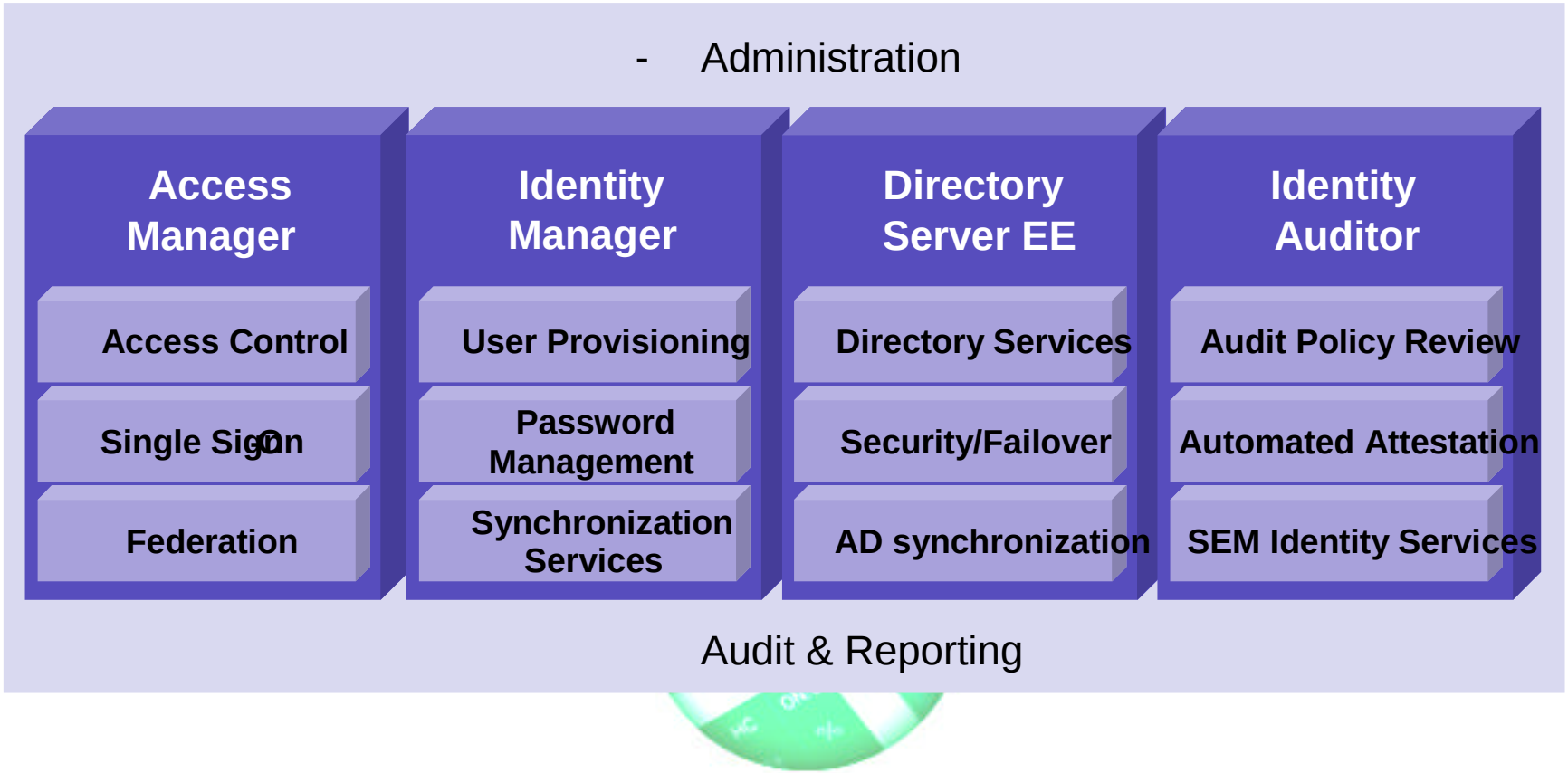


Comment ca marche ?

Jean-Paul Bembaron

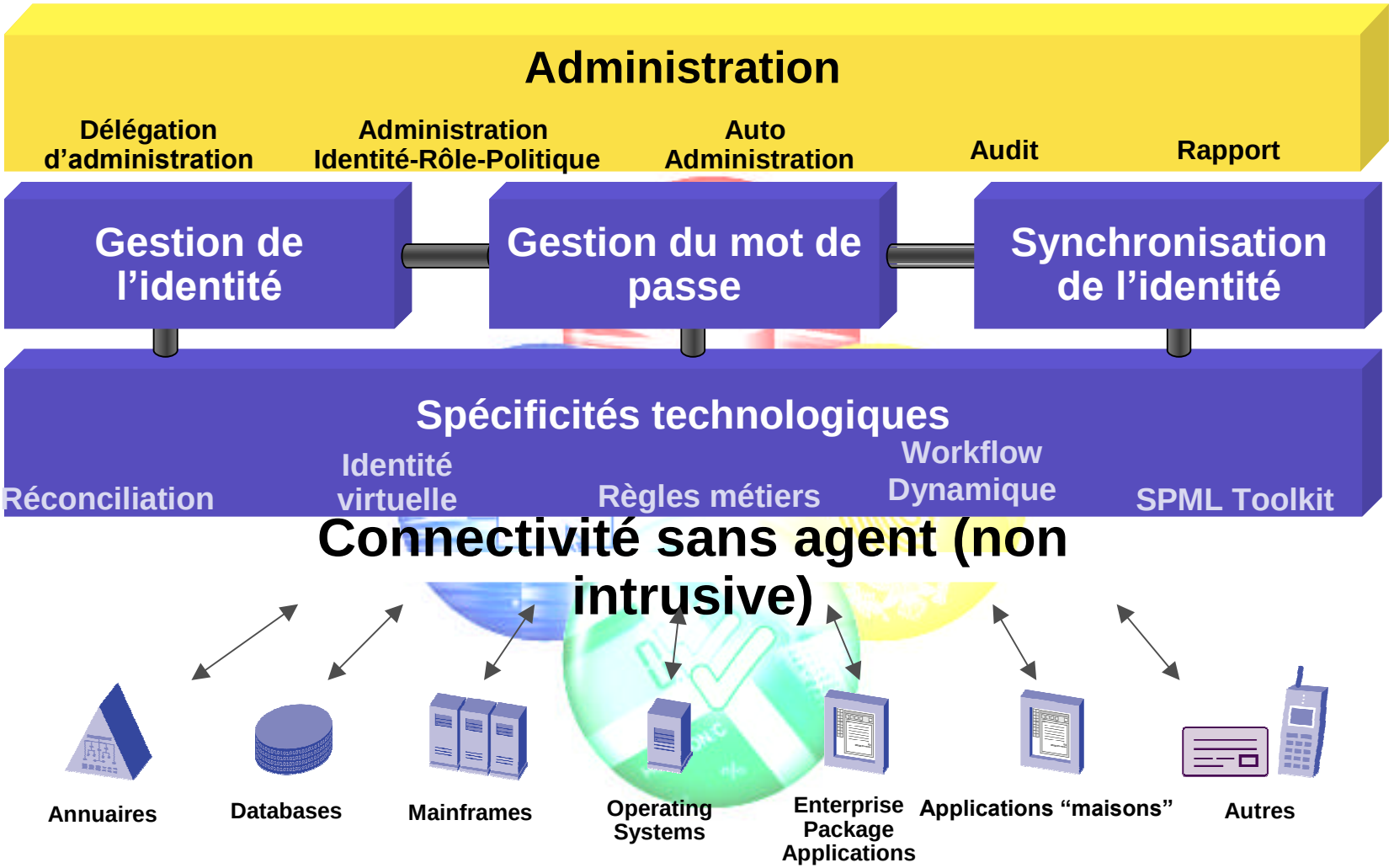
Sun Microsystems France

La vision fonctionnelle de la Gestion de l'identité :

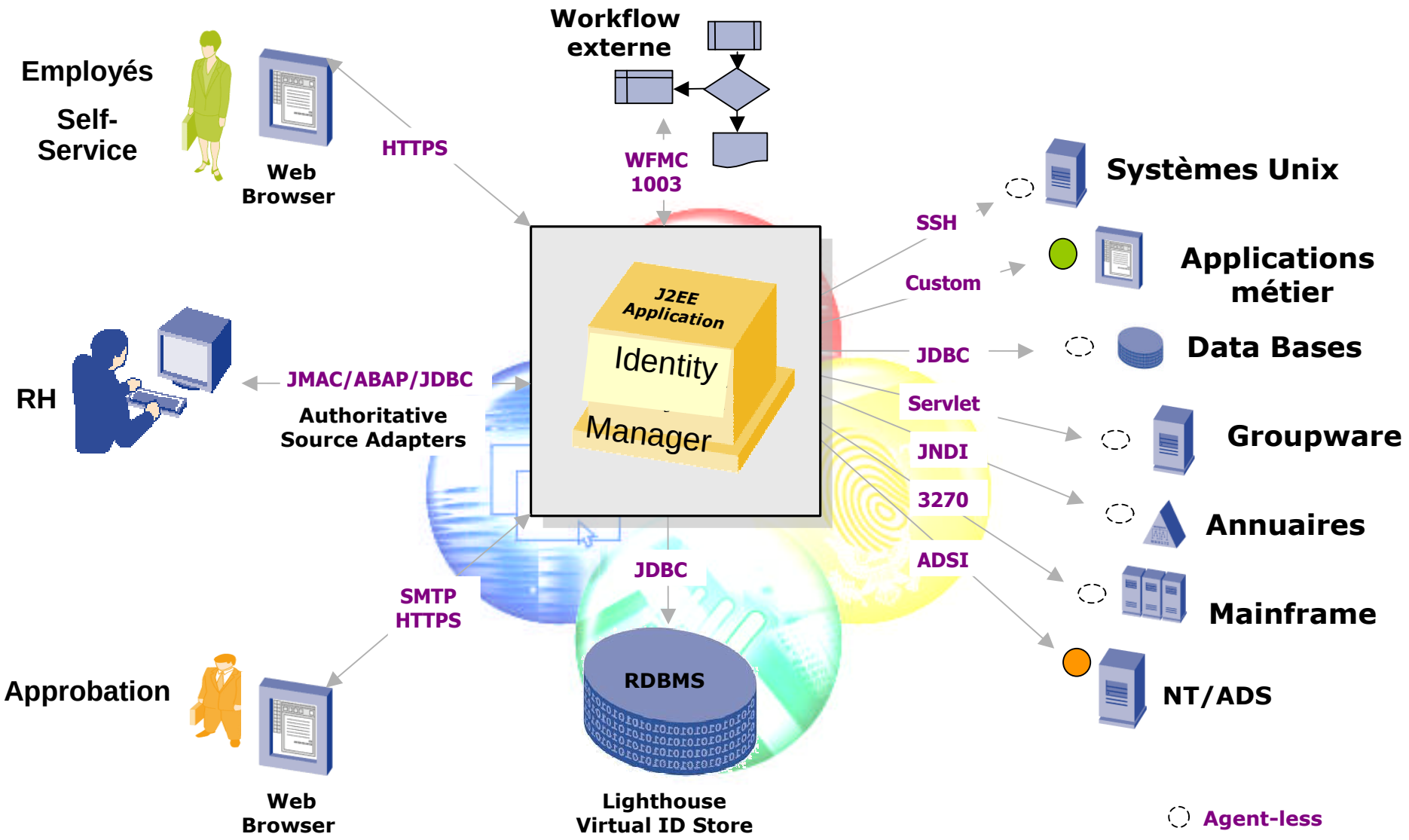


Composant par composant

Sun Java System Identity Manager

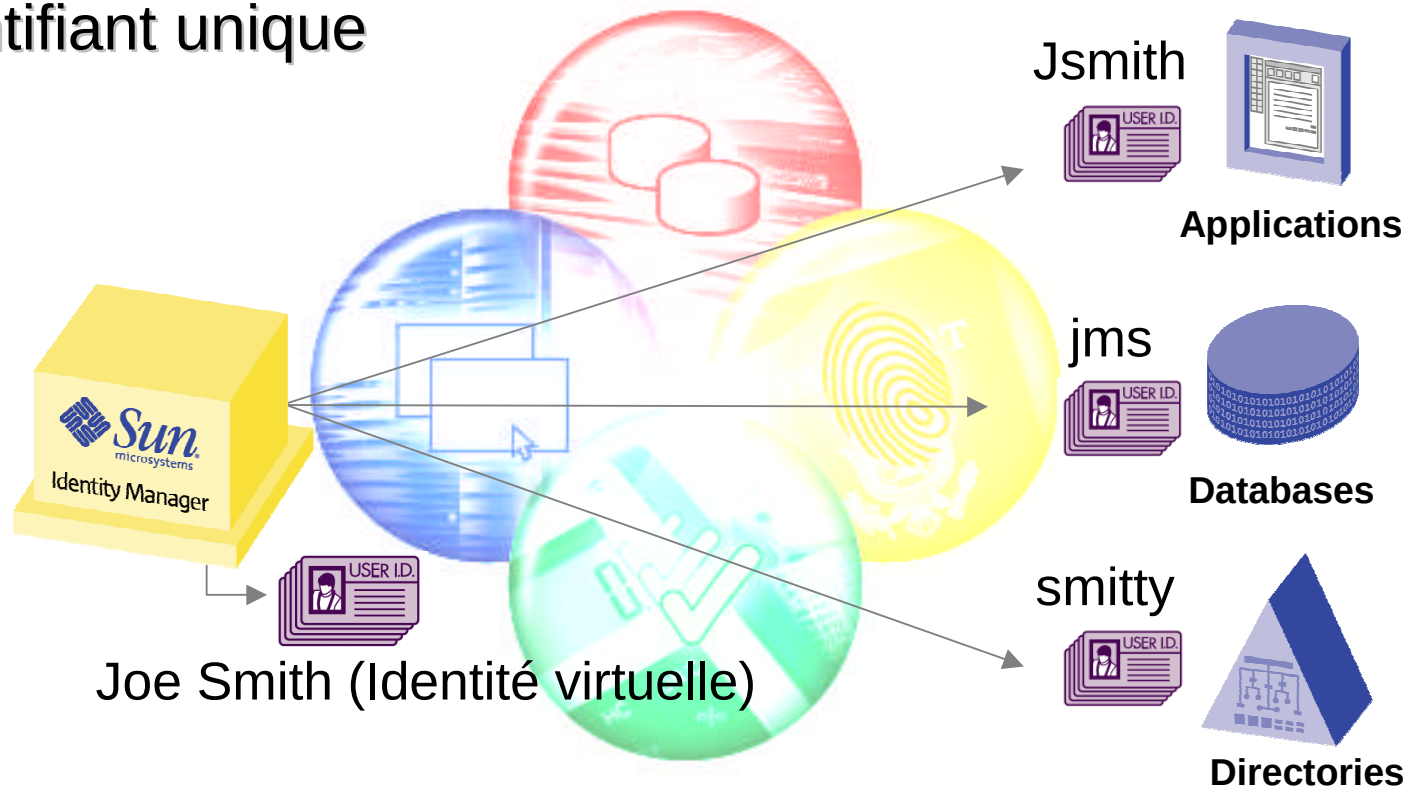


Architecture Technique



Spécificités technologiques

- Identité virtuelle et temps réel
  - Gestion logique d'identités multiples
  - Gestion des comptes ”orphelins”
  - Identifiant unique



Automating the Provisioning Process…

System A	System B	System C	System D	System E	System F
Jberry	Bbanks	A49320	Cooperl	Skeeti	Sequensh
Esiegel	Lsulley	A39943	Tinleyj	Frenetc	Welchj
Jrowland	Lbitmore	A49454	Harrisd	Smileys	Pettyr
Mfriedel	Ltimble	A93934	Mcquittyp	Entrald	Robertsj
Sbenson	Aboyle	A39485	Rowlandr	Novacho	Julianr
Thanks	Bcoldwel	A49382	Bensons	Alvarag	Nantpre
Jwayne	Dparis	A48382	Quinleys	Narlersh	Enaget
Tcarrol	Clriot	A49382	Harminb	Woodst	Jhancock
Sharris	Etear	A39485	[redacted]	Nicklausj	Johnh
Bwhite	Smackay	A29483	Francek	Hoganb	Hanwayv
Ddailey	Mturner	A49583	Lipperd	Palmera	Composi
Eheiden	Mmclain	A49382	Skatee	Dimarcoc	Initalial
Lball	Mcpasch	A49302	Marinoe	Perryk	Pmcquitty
Hwiggins	Jpasch	A42845	Flamingo	Beards	Stickler
Cjohnson	Philm	A20184	Russiak	pdm33	Bourne
Cwillis	Tdean	A49284	Crowd	Fusar	Fusar
Pmcquitty	Jtorville	A49248	Pazzaz	Poli	Margoliao
Mthomas	Cdean	[redacted]	Daoudc	Margaglio	Navka
Browland	Nreagan	A42948	Louf	Lithowan	Koskoma
Mprehn	Rnixon	A49274	Peizerat	Vanagas	Hackinsa
Ggoodnow	Gbush	A37520	Anissina	Lightes	Newjers
Slake	Jvance	A49294	Ferrisb	Naugano	[redacted]
Bblake	Jcarpent	A03749	Lupers	Footman	Alexander
Fjohnson	Mstewart	A49274	Lobach	Figureas	Sasha
Galonso	Lchristia	A33993	Frenchj	Lupesh	Reuben
Slippes	[redacted]	A38288	Navratol	Arganish	Struedl
salger	jmackay	A48228	dellm	Delegant	tangor
ralnc493	ralnc493	ralnc493	ralnc493	ralnc493	ralnc493

Identity Management

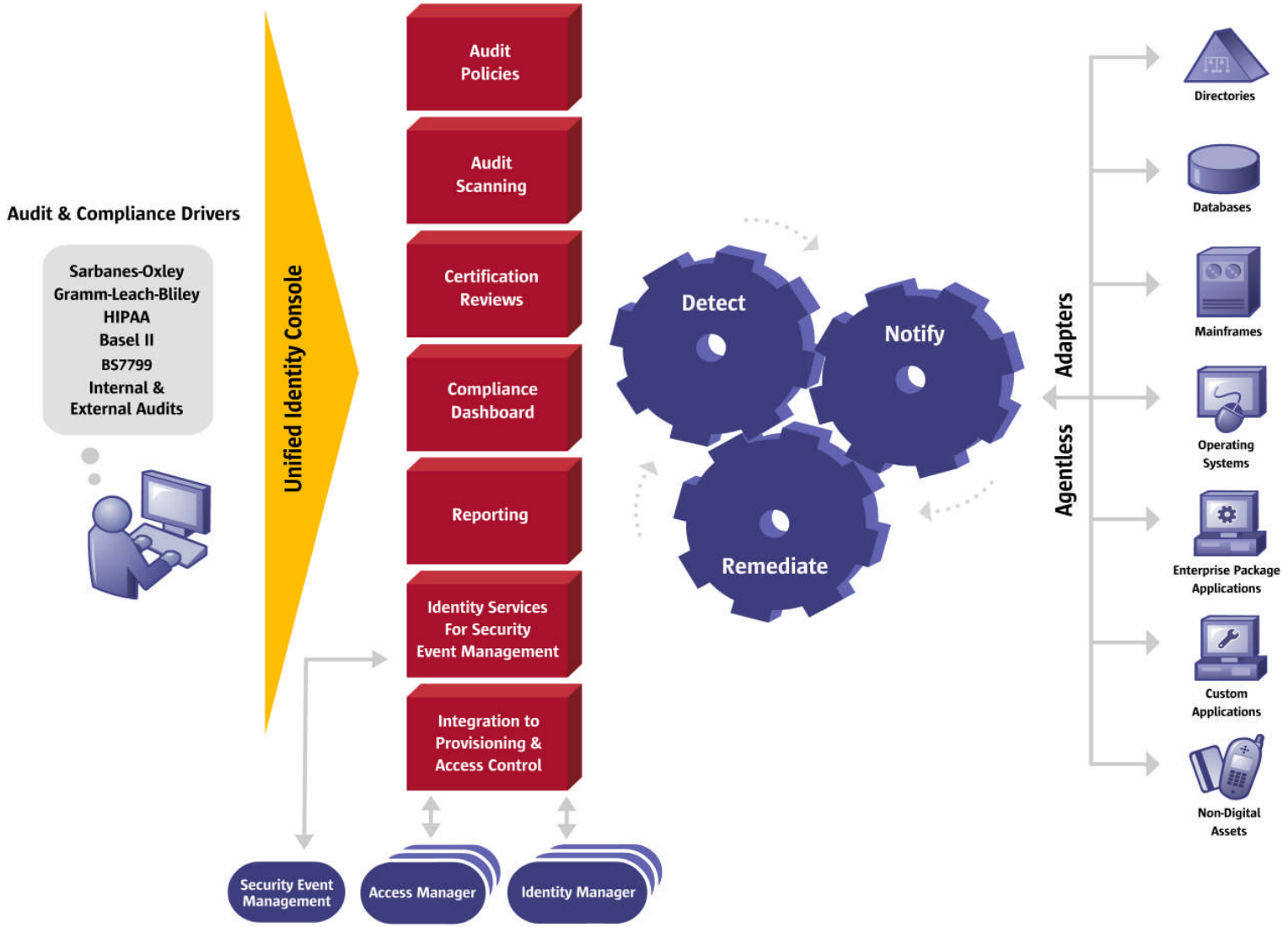
- Account Discovery
- Account Mapping
- Account Provisioning
- Account Risk Analysis
- Password Change / Sync
- Account Disable / Removal

The Solution Must Provide

- Central Audit Trail / Accountability
- Secure Delegation of Administration
- Automated Workflow / Approvals
- Security Policy Enforcement
- Standards-based Interfaces

- SystemA Pmcquitty
- SystemB Philm
- SystemC A49382
- SystemD Mcquittyp
- SystemE pdm33
- SystemF pmcquitty

Identity Auditor



Le support d'applications hétérogènes

Messageries
- Lotus Notes 5.0 (Domino)
- MS Exchange
- GroupWise

Annuaires
- LDAP
- Sun ONE™ Directory Server (iPlanet)
- MS Active Directory (idem W2K)
- Novell

Help Desk
- Remedy Help Desk

Systèmes d'exploitation
- HP-UX
- IBM AIX
- IBM OS/400
- Microsoft
- Redhat Linux
- Sun Solaris
- VMS

Applications métier - ERP
- Peoplesoft
- SAP
- Siebel

Bases de données
- DB2 Universal Database for UNIX, LINUX, Windows
- MS SQL Server
- MySQL
- Oracle
- Sybase

Gestion de la sécurité
- eTrust CA
- IBM RACF
- Entrust® Authority™ Security Manager
- RSA SecurID

Gestion des accès
- IBM/Tivoli Access Manager
- Netegrity Siteminder Admin
- SunONE ID Server
- Entrust GetAccess™
- RSA ClearTrust

Références


Sun microsystems
The Federal Reserve Board
KRAFT
Gap Inc.
Gap
Banana Republic
Old Navy
Deutsche Bank
ProBusiness
BNSF
Burlington Northern Santa Fe Railway
UNION PLANTERS CORPORATION
DELL
SONY
AMGEN
AdvancePCS
WELLPOINT
HM Customs and Excise
USG
HITACHI
Inspire the Next
Unilever
Henkel
A Brand like a Friend
Circuit City
BANCADEL GOTTARDO
ADP
BlueCross BlueShield Association
Jim Beam
Pfizer
PACIFICORP
Allianz
GUIDANT
Seagate
We turn on ideas
CONSECO
Step up
Standard Chartered
NOVARTIS
DYNEGY
Gap Inc.
DTE Energy
Detroit Edison
Philip Morris USA
ppl
Freddie Mac
LOCKHEED MARTIN
We never forget who we're working for
Merrill Lynch
'yes' OPTUS
TELECOM ITALIA

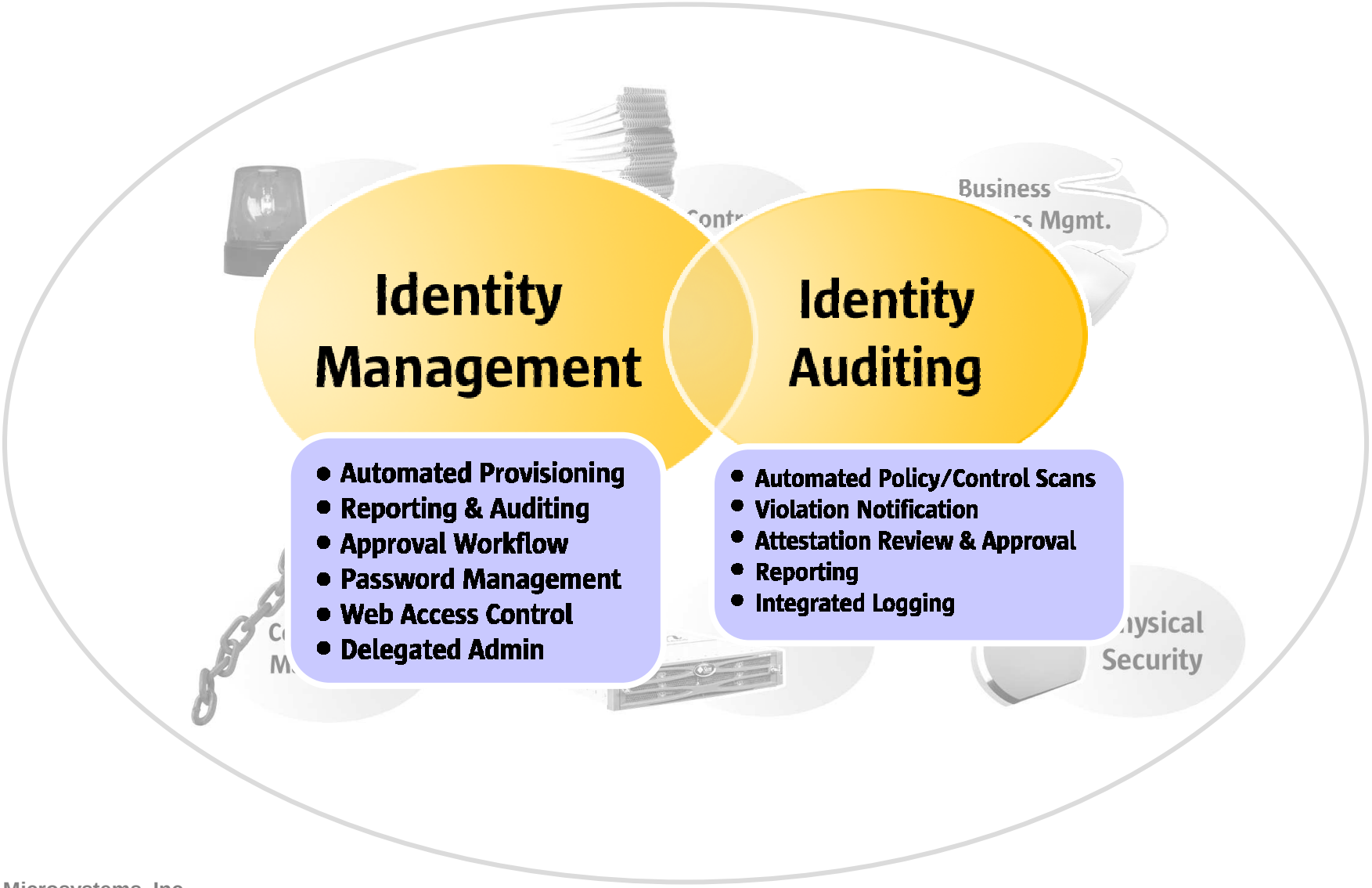
Témoignage client

Monsieur Provost – Gie Carte Bancaire

Sun microsystems

We make the net work.

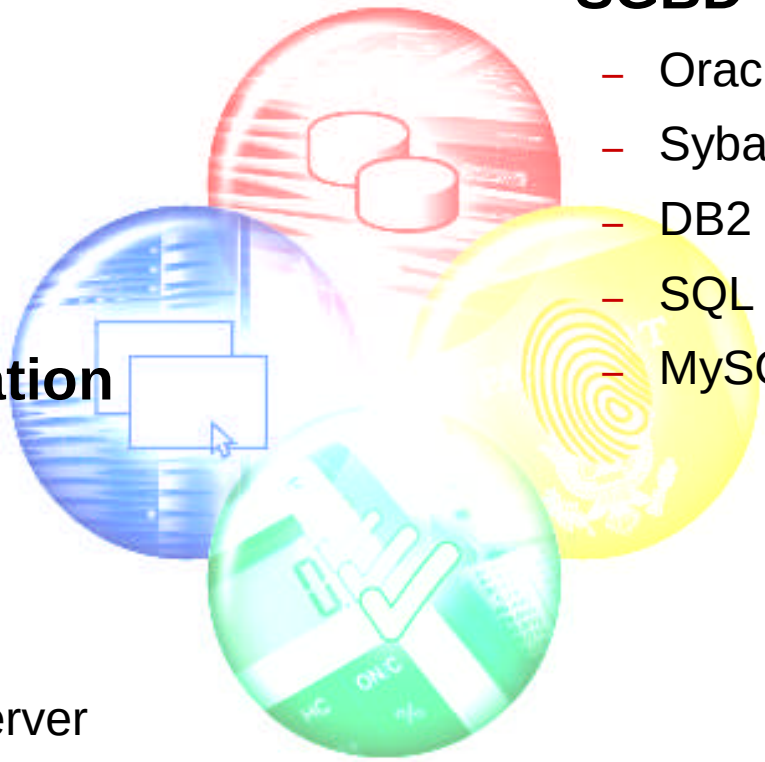
Périmètre Technologique de Conformité



Architecture technique

- **Système d'exploitation**
  - IBM AIX
  - HP-UX
  - Windows
  - Red Hat Linux
  - Solaris

- **Serveur d'application**
  - BEA Weblogic
  - IBM Websphere
  - Tomcat
  - Sun Application Server



- **SGBD**
  - Oracle
  - Sybase
  - DB2
  - SQL Server
  - MySQL