# La gestion d'identités: une nécessité sur les campus Numériques

Marie-Francoise Penta /Olivier Prompt

Manuel Jaffrin

Sun microsystems

# Agenda

- Introduction et définition des concepts de la gestion intégrale d'identités numériques
- Les grandes étapes de la mise en place d'une solution globale
- Les solutions Sun – Démonstration - Discussion
- Quelques exemples de projets en cours
- Vers un model Fédéré - Conclusion

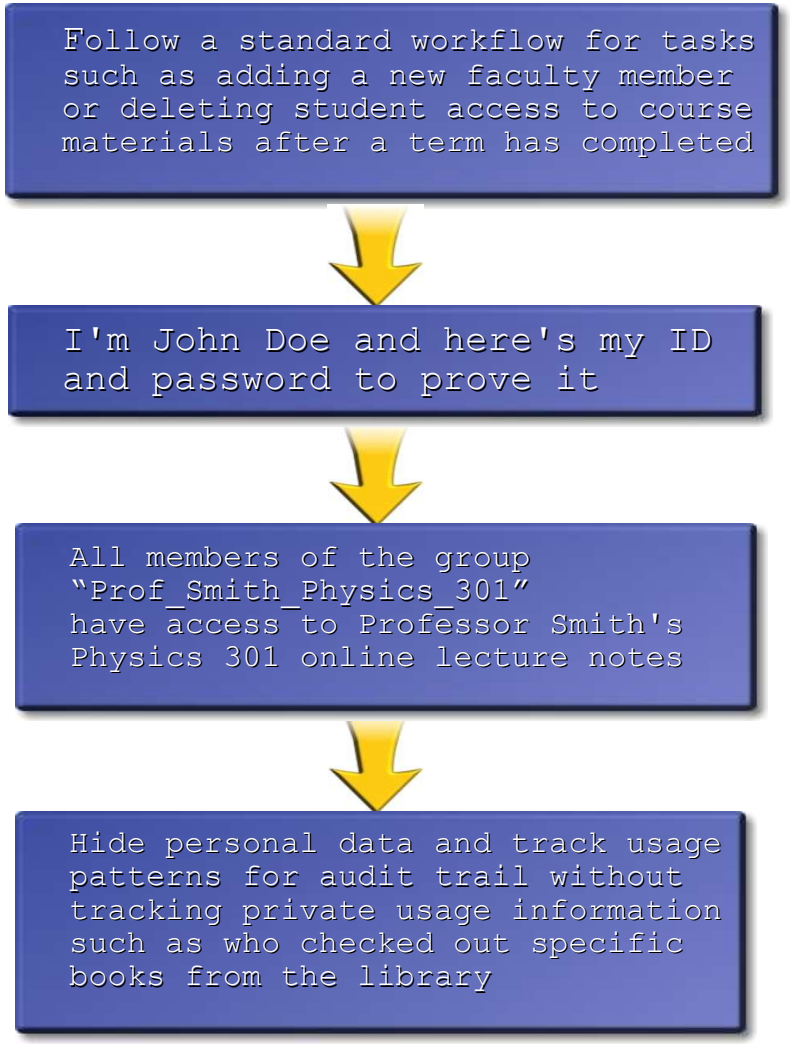
# Quelle définition pour la gestion de l'identité numérique ?

*"La gestion des identités Numériques est la combinaison d'un ensemble de processus et d'une infrastructure technologique pour la création, la maintenance et l'utilisation de ces identités."*

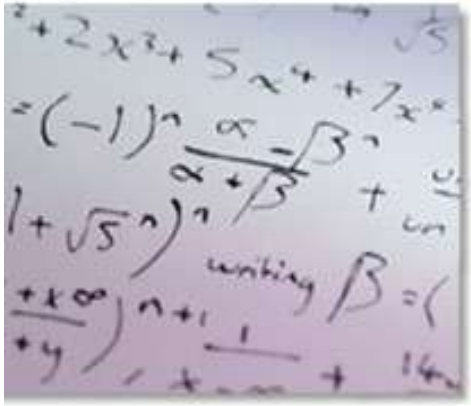
–The Burton Group

# Les grandes fonctions de la gestion d'identités

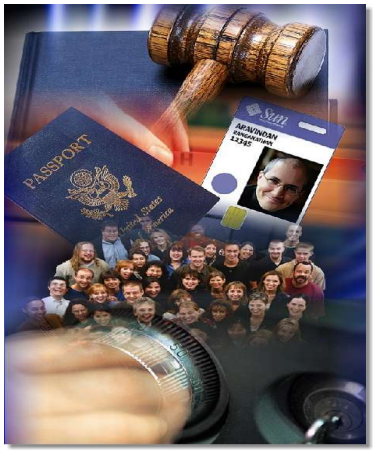
- *Provision d'accès & Propagation* Création, modification des comptes et privilèges des utilisateurs
- *Authentification* Confirmation de l'identité de l'utilisateur
- *Authorisation* Autorise l'accès aux services et ressources en fonction de règles et roles
- *Protection des données et conformité avec les lois*



# Des besoins et des environnements très complexes



- Très grande nombre “d'utilisateurs”
- De nombreux roles:
  - Des besoins d'accès différents
  - Les utilisateurs ont souvent de multiples roles
  - Ces roles changent fréquements
- Environnemt Multi-campus (Collaboration)
- Existance de multiples base de données d'identités fragmentées
- Nécessité de mettre en place une politique de Sécurité globale



# Le cycle de vie des identités sur un Campus

- Faculty member leaves
- Student graduates or drops out
- Research contracts expire
- Non-digital resources retrieved and/or canceled


- User info entered via student admissions, faculty hiring, etc.
- Accounts provisioned to enterprise systems, applications, directories
- Non-digital resources assigned and/or initiated

- Faculty job/role/status changes
- Student classes change at end of term
- Password changes and resets
- Profile or contact information changes
- Additional requests for account access or non-digital resources

# Les grandes étapes pour l'implémentation d'une solution globale

# Etape 1 – Services d'authentification centralisés

**Permet le Single Sign-on entre les applications connectées**

- *Les Applications ont accès* aux meme services centraux d'authentification
- *Support du single sign-on* – Web Initial Sign-On (Web ISO)

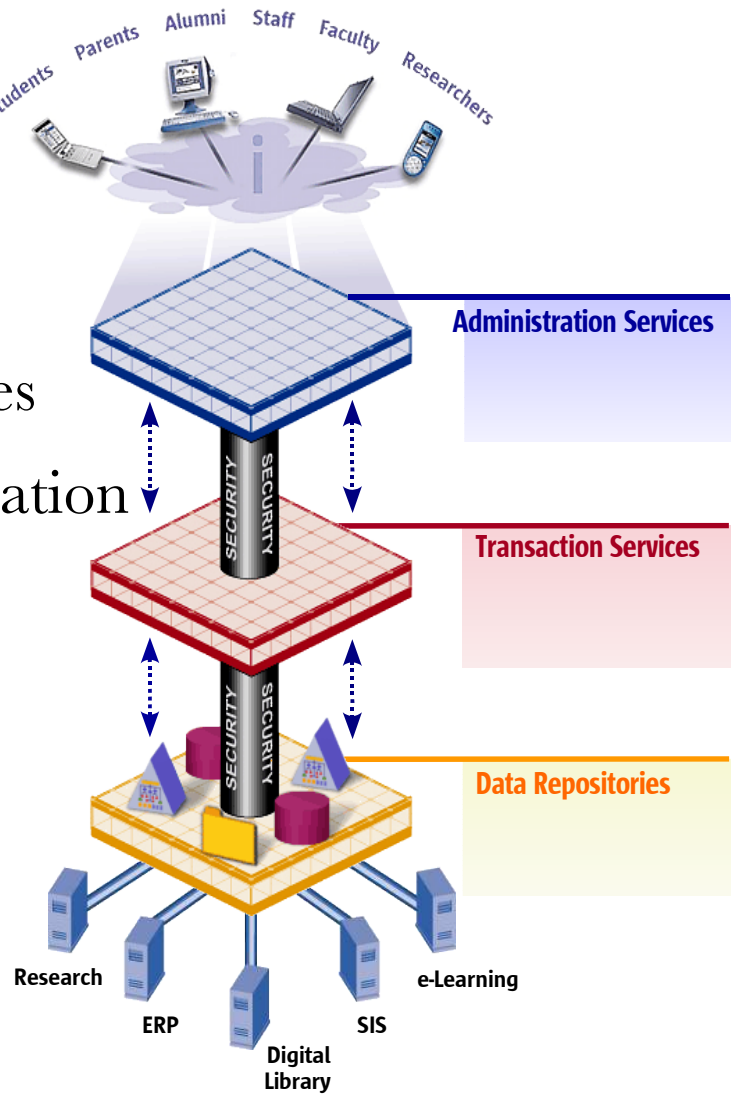
# Etape 2 – Services d'autorisation centralisés

**Permet la gestion centralisée des droits d'accès**

- *Les Applications ont accès* à un service centralisé d'autorisation basé sur des roles et profiles
- *Extension vers un modèl fédéré* pour simplifier la collaboration entre institution

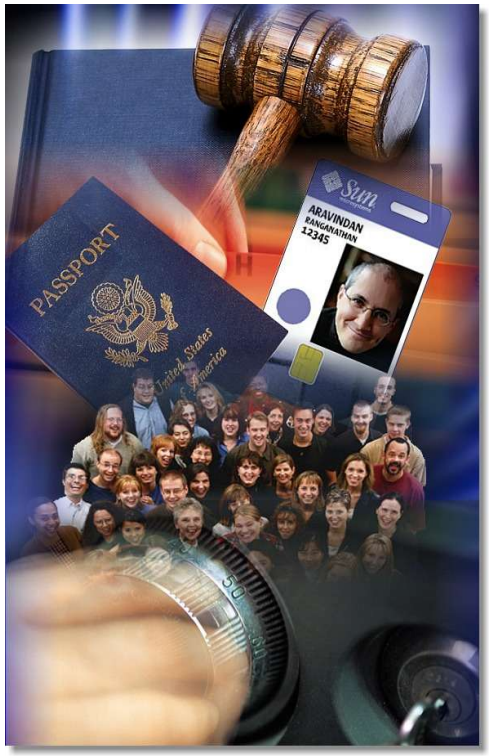
# Etape 3 – Gestion total automatisée

- Automatisation des flux d'information
- Autorisation basée sur des roles et règles
- Sistème globale d'audit et de monitorisation
- Gestion autonome des mots de passe
- Fédération des identités

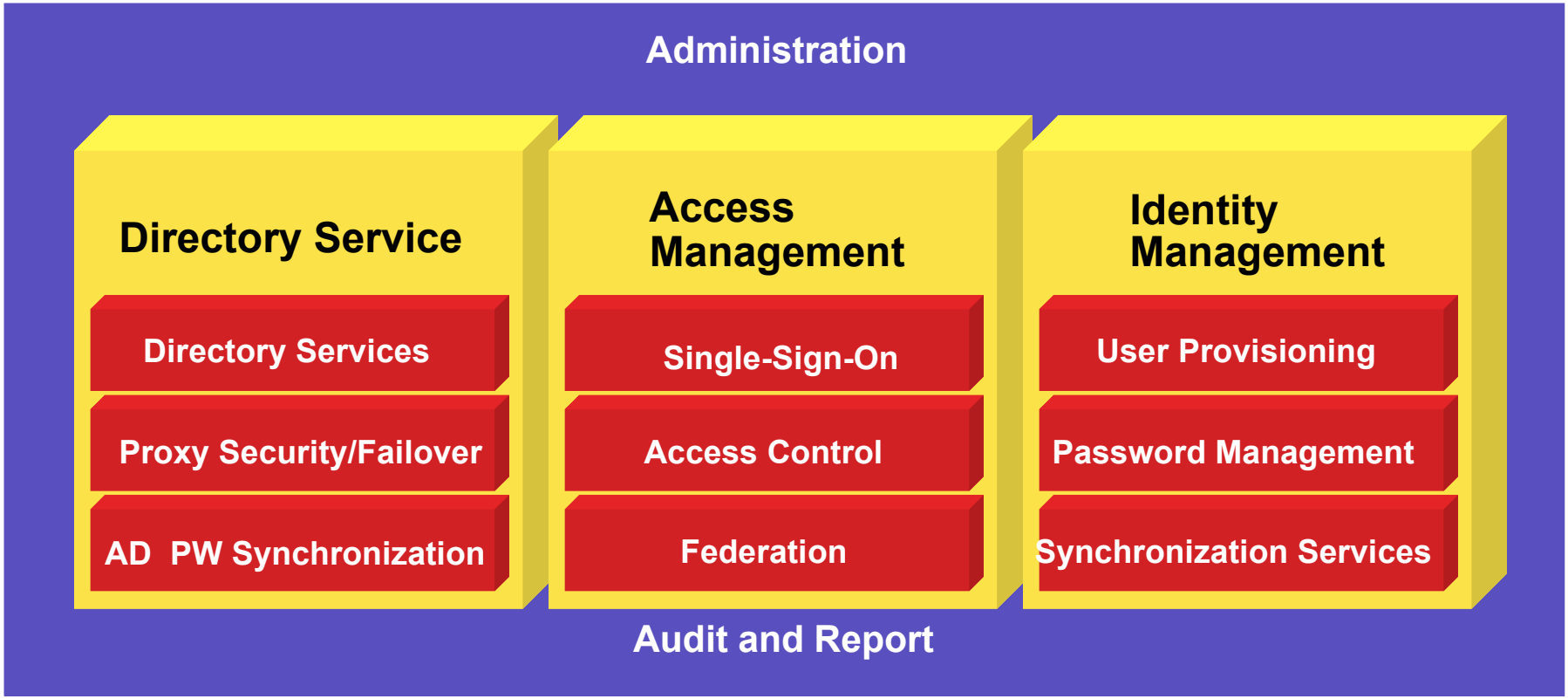


# Les avantages d'une solution globale

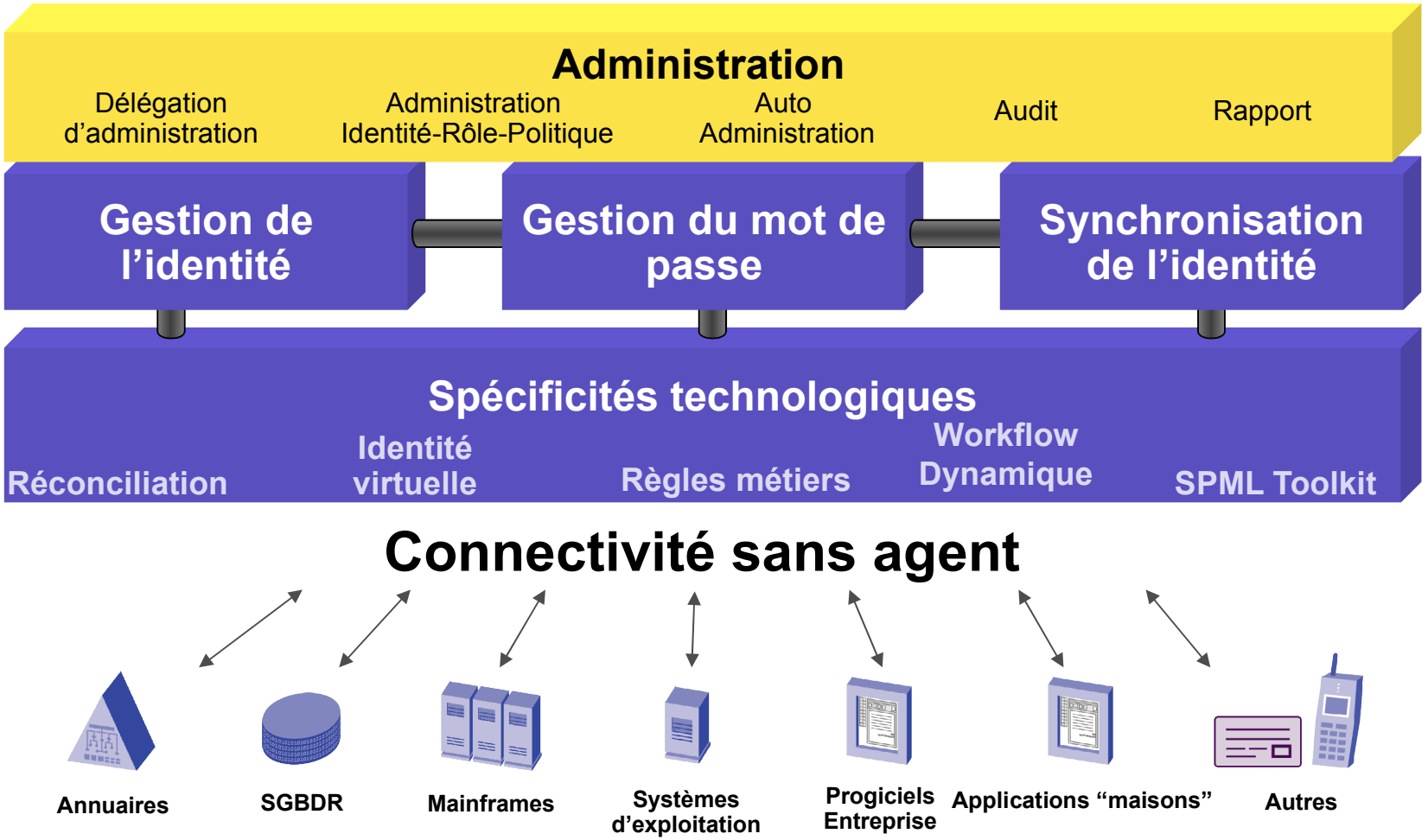
- Meilleure sécurité
- Capacité de monté en charge et réduction des couts/complexité
- Efficacité / Productivité
- Meilleure qualité de service
- Fédération
- Possibilité accrue de collaboration entre institutions



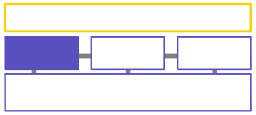
# Le socle de Sun:
# Java Enterprise System
# Identity Management Suite


Administration
Directory Service
Directory Services
Proxy Security/Failover
AD PW Synchronization
Access Management
Single-Sign-On
Access Control
Federation
Identity Management
User Provisioning
Password Management
Synchronization Services
Audit and Report

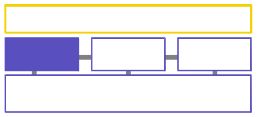
# Démonstration Identity Manager



# Gestion d'Identité



# Gestion d'identité : constat



Partenaires

Employés

Clients

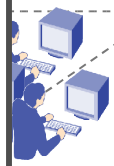
Anciens Employés/pr estataires

Où sont les risques?

Qui accède à quoi ?

Quelles sont les tâches répétitives et coûteuses ?

Quel est le coût de cette gestion fragmentée ?



Centre de support

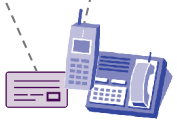
Help Desk

Gestion des équipements

Exchange/Active Directory

Oracle Finance

Siebel CRM



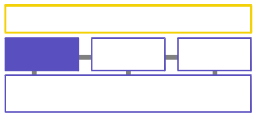
Équipements

- Téléphone mobile
- Compte de Conf. Call
- Carte de crédit

Autres équipements

- Bureau
- Téléphone
- Portable

# Gestion d'identité : proposition de Sun



Partenaires

Responsable RH

Employés

Clients

Anciens employés/prestataires

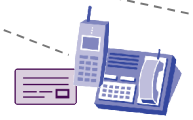
- Réduction des risques
- Vue globale de l'identité d'un utilisateur
- Efficacité et automatisation


Approbation hiérarchique

Exchange/Active Directory

Oracle Finance

Siebel CRM



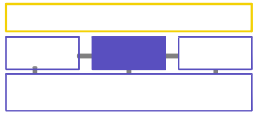
**Équipements**

- Téléphone mobile
- Compte de Conf. Call
- Carte de crédit

**Autres équipements**

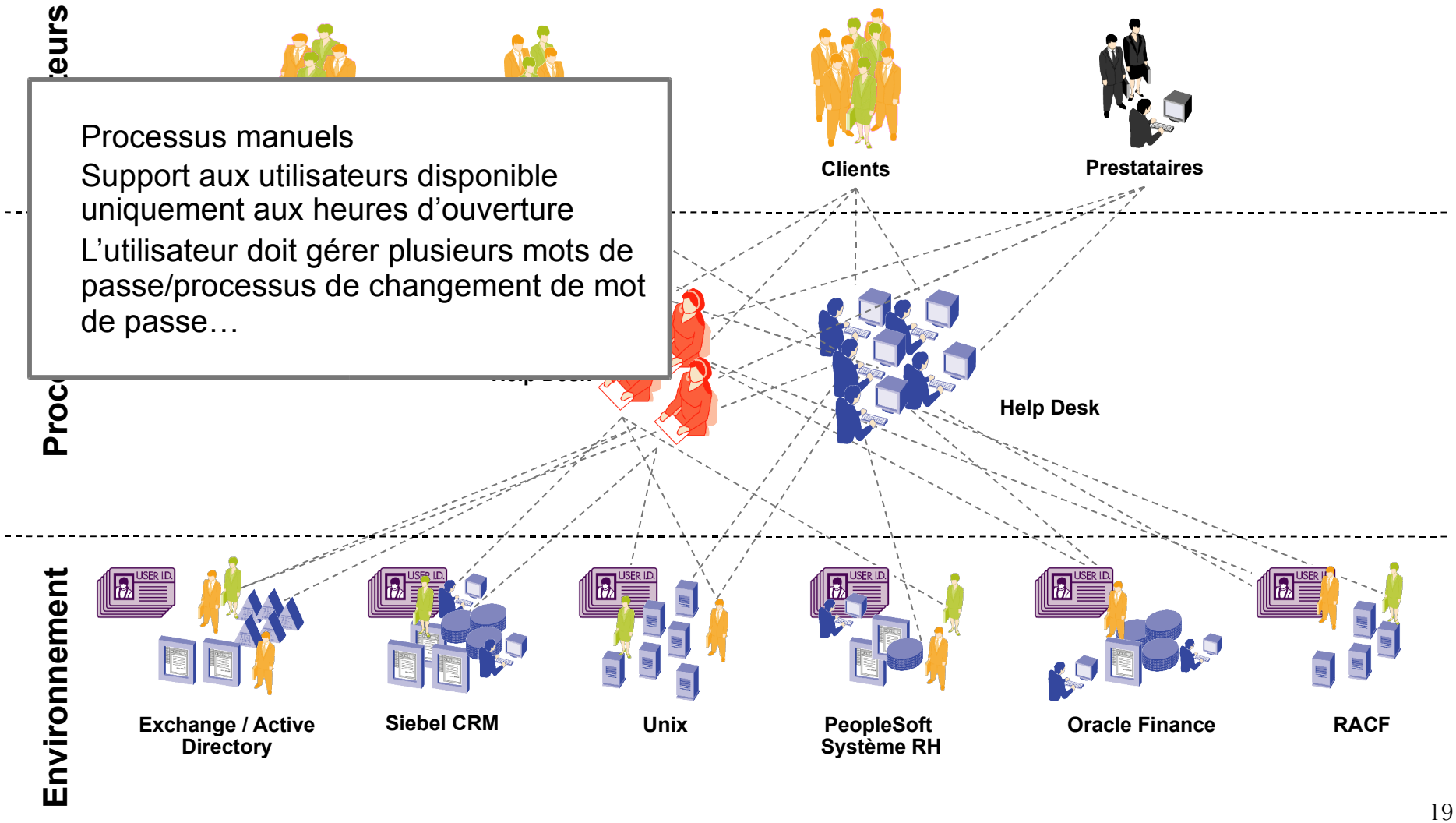
- Bureau
- Téléphone
- Portable

# Gestion du mot de passe

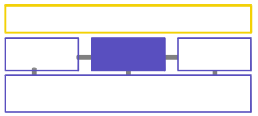


# Gestion du mot de passe : constat

Processus manuels
Support aux utilisateurs disponible uniquement aux heures d'ouverture
L'utilisateur doit gérer plusieurs mots de passe/processus de changement de mot de passe…



# Gestion du mot de passe : apports SJSIM



Utilisateurs

Processus

Environnement

Partenaires

Employés

Clients

Prestataires

Sun microsystems Identity Manager

Automatisation des processus de changement du mot de passe

Disponible en permanence

Un seul point central de gestion

Exchange / Active Directory

Siebel CRM

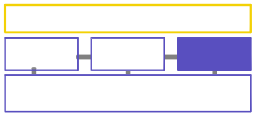
Unix

PeopleSoft Système RH

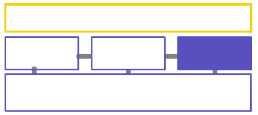
Oracle Finance

RACF

# Synchronisation



# Les besoins de synchronisation

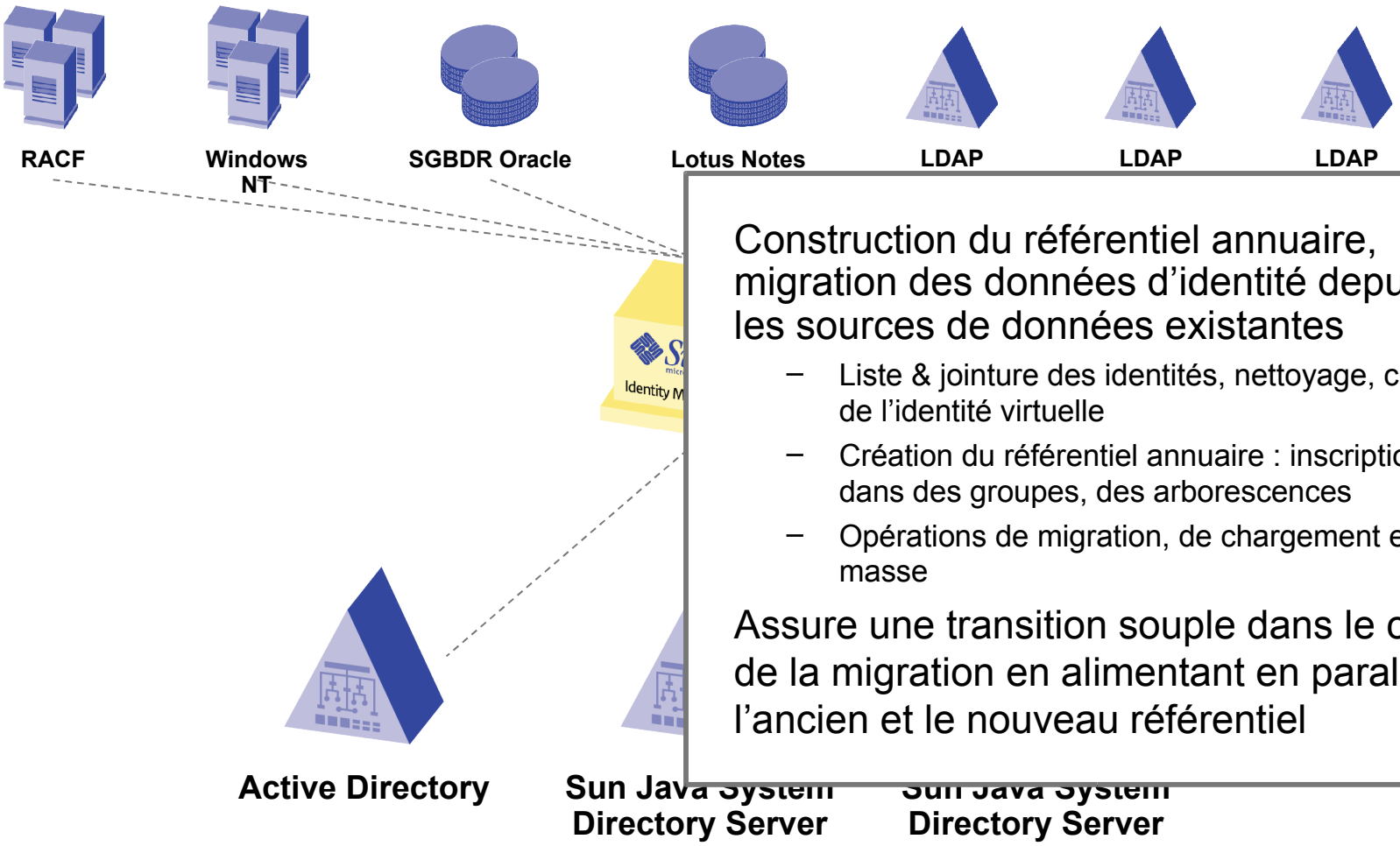


Migration vers une infrastructure d'annuaire

Garantir la cohérence des données d'identité dans le référentiel et dans les applications concernées

- Gestion des profils et des droits d'accès
- Gestion de la synchronisation de donnée

# Synchronisation : Identity Manager

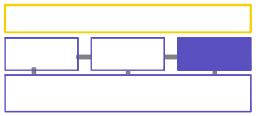



Construction du référentiel annuaire, migration des données d'identité depuis les sources de données existantes

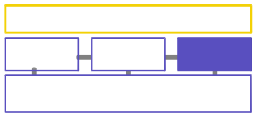
- Liste & jointure des identités, nettoyage, création de l'identité virtuelle
- Création du référentiel annuaire : inscription dans des groupes, des arborescences
- Opérations de migration, de chargement en masse

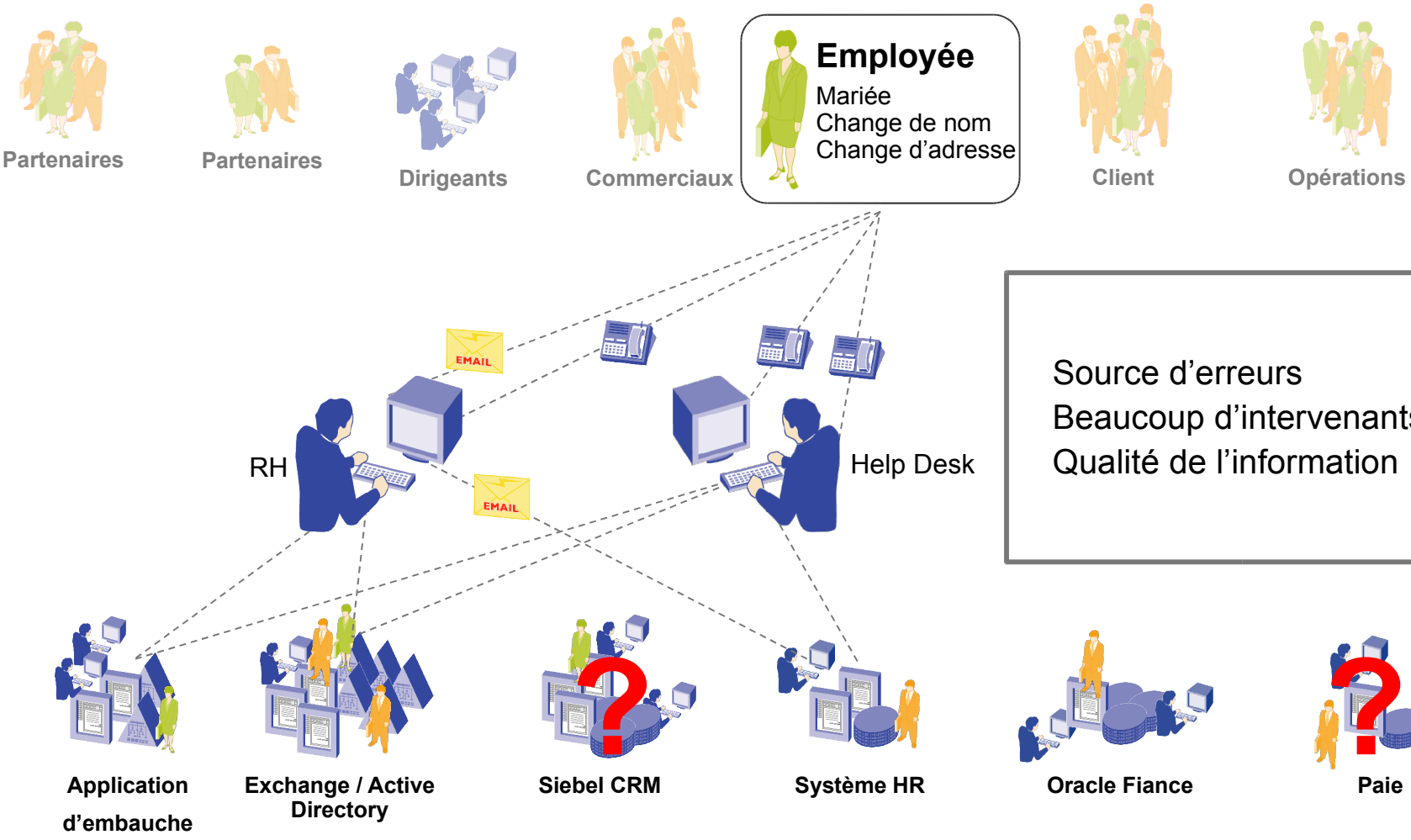
Assure une transition souple dans le cadre de la migration en alimentant en parallèle l'ancien et le nouveau référentiel

# Gestion des profils et des changements

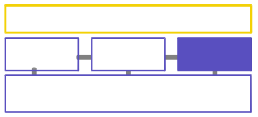


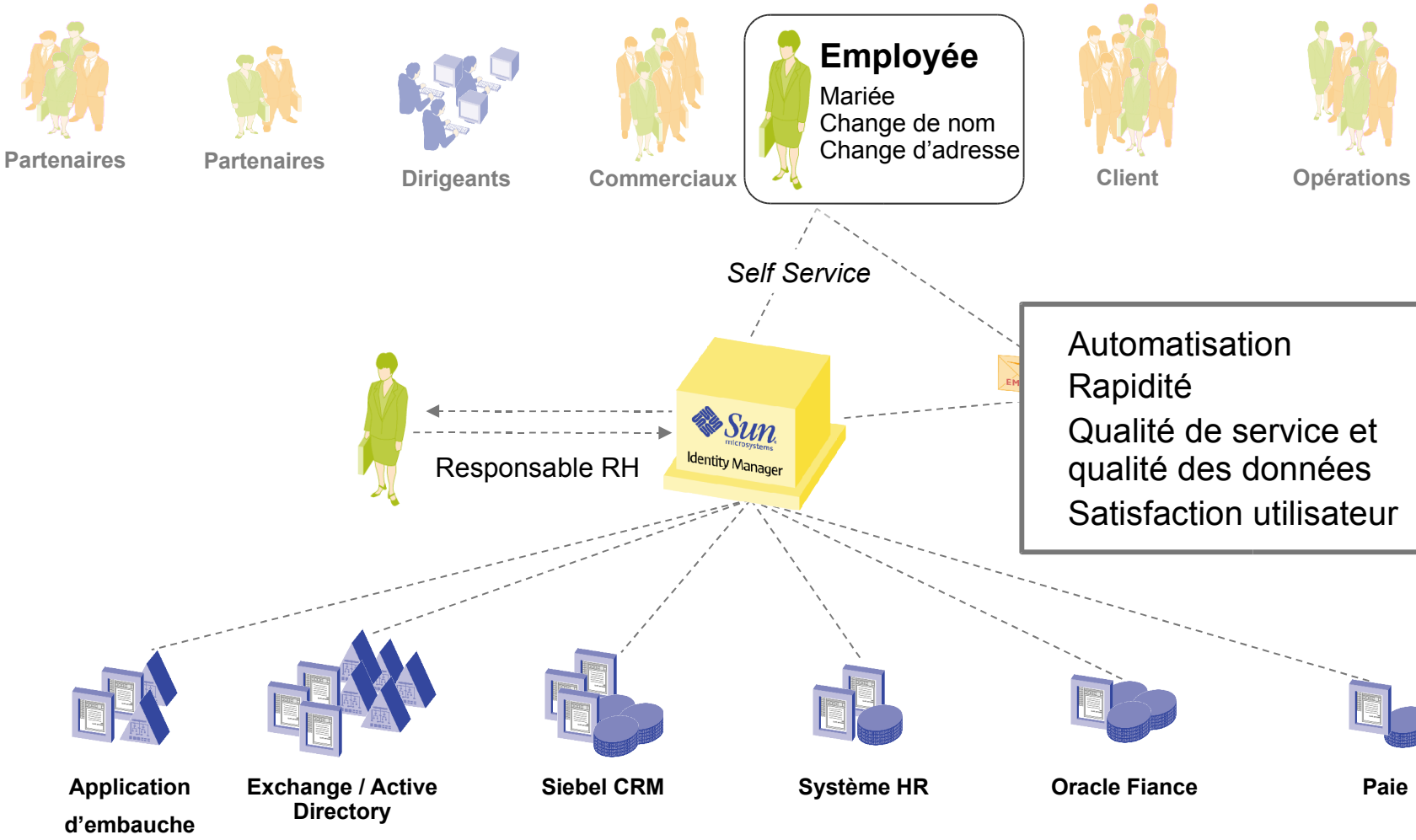
# Gestion de profils : constat



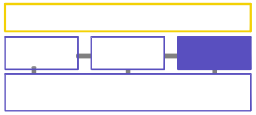


# Gestion de profils : apports





# Administration



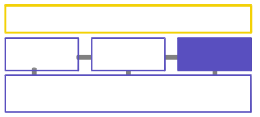
# Administration : constat

Les sources de données sont souvent la propriété individuelle d'un service et administrées manuellement

Les mises à jour manuelles sont source d'erreurs et de perte de temps

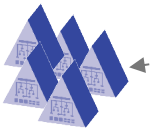
Risques importants d'incohérences de l'information d'identité dans les différents systèmes

# Administration centralisée : apports



Modification **Département, Job Code, Titre** pour les pages blanches


Une promotion
- Nouveau **Titre**
- Nouveau **Job Code**
- Nouveau **Coefficient**
- Nouveau **Département**



**Annuaire d'entreprise**

**Exchange / Active Directory**

**Système RH**

**ERP**

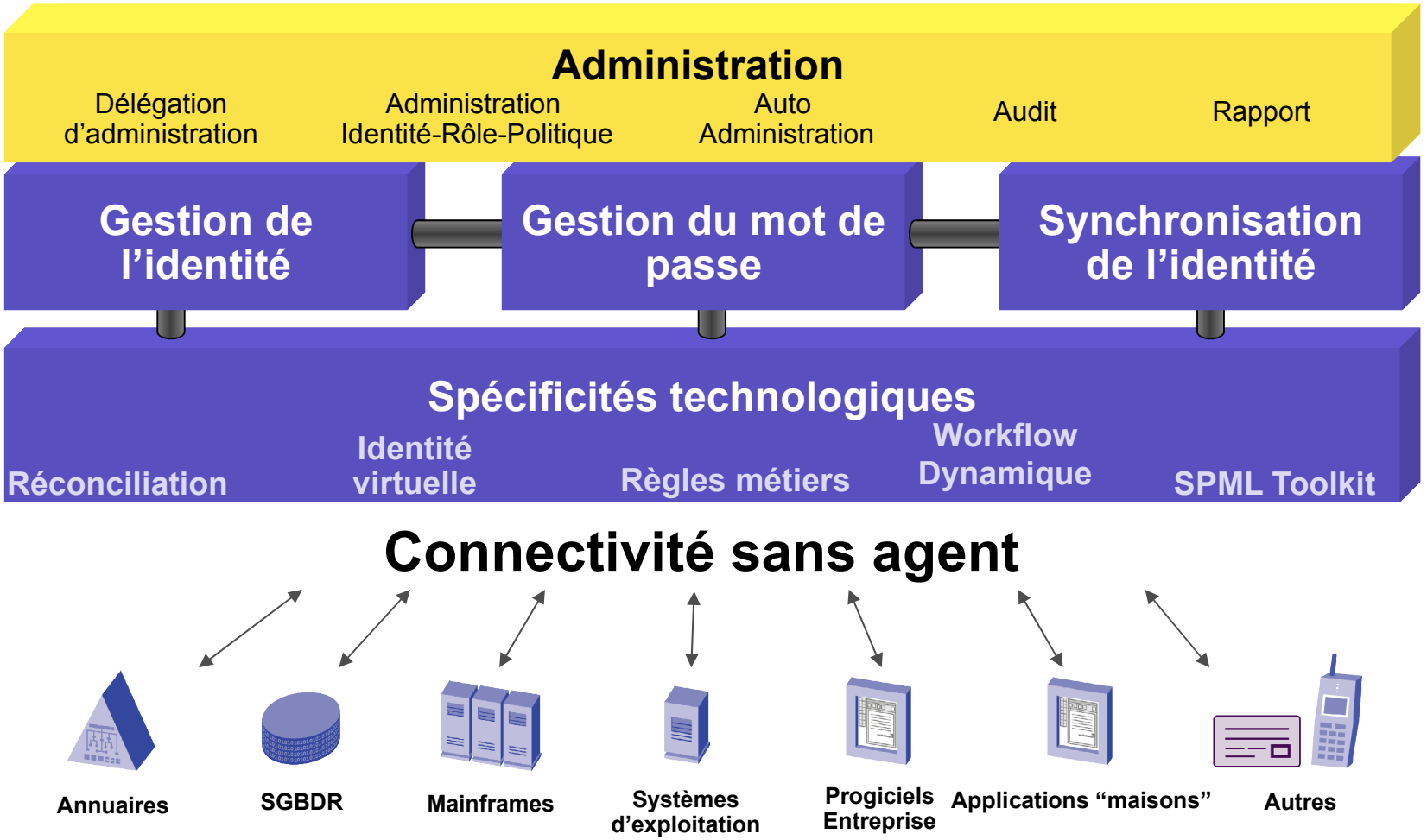
**Système de paie**

Modification du **Coefficient** pour révision du salaire de base

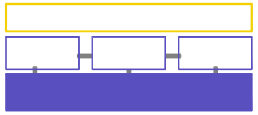
- Modification du **Job Code**
- Modification des accès

- Modification du **Département, Titre, Job Code**
- Modification home directory et déplacement des fichiers
- Modification du message 'db account size' pour l'employé

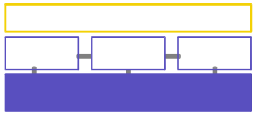
# Sun Java System Identity Manager



# Spécificités technologiques



# Les services d'Identity Manager



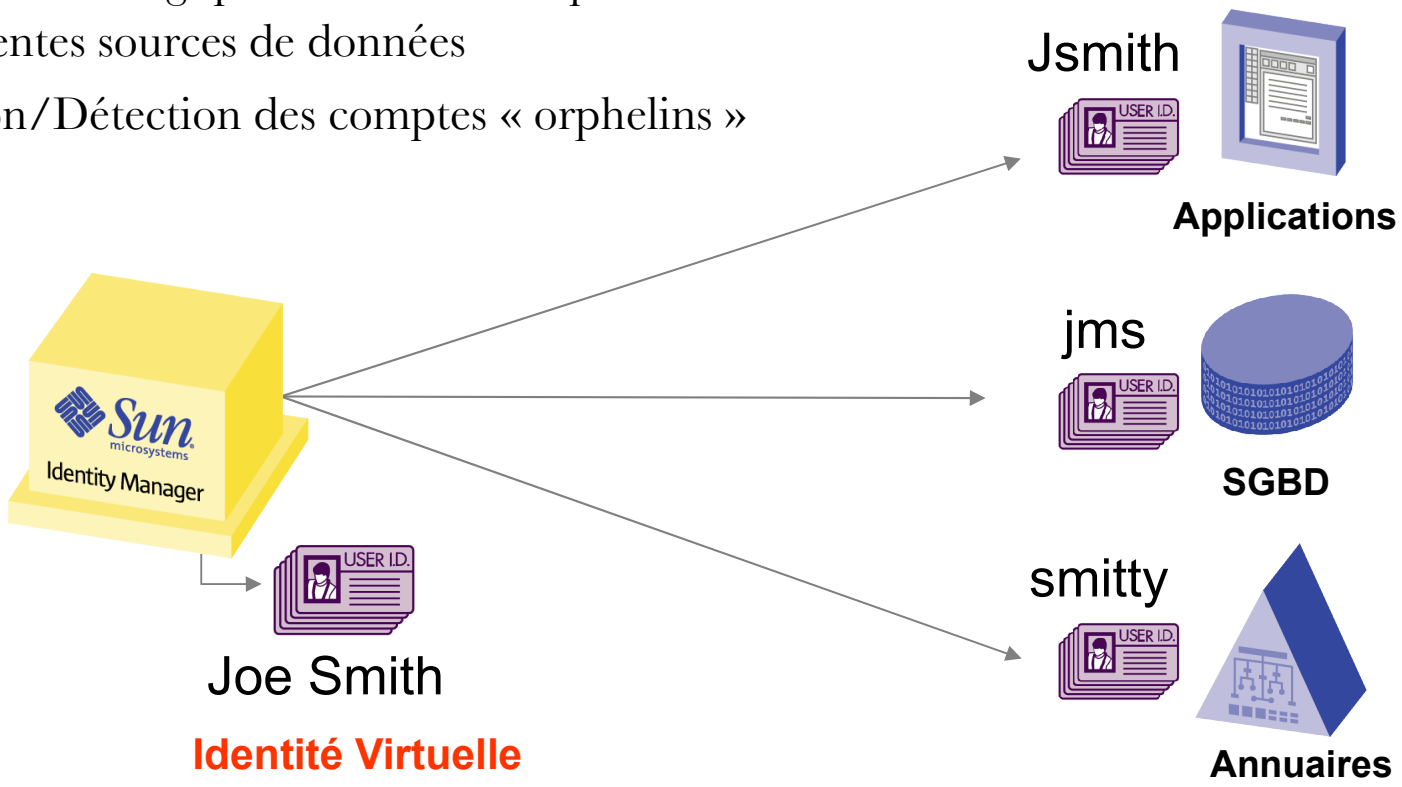
Une approche non intrusive pour faciliter le déploiement et améliorer la gestion de l'identité

- Moteur de règles
- Workflow dynamiques
- Auto-discovery
- Gestionnaire d'Identité virtuelle
- Adaptateurs de ressources « sans agent »

# Spécificité technique : Identité virtuelle

Représentation logique des identités réparties dans les différentes sources de données

Réduction/Détection des comptes « orphelins »

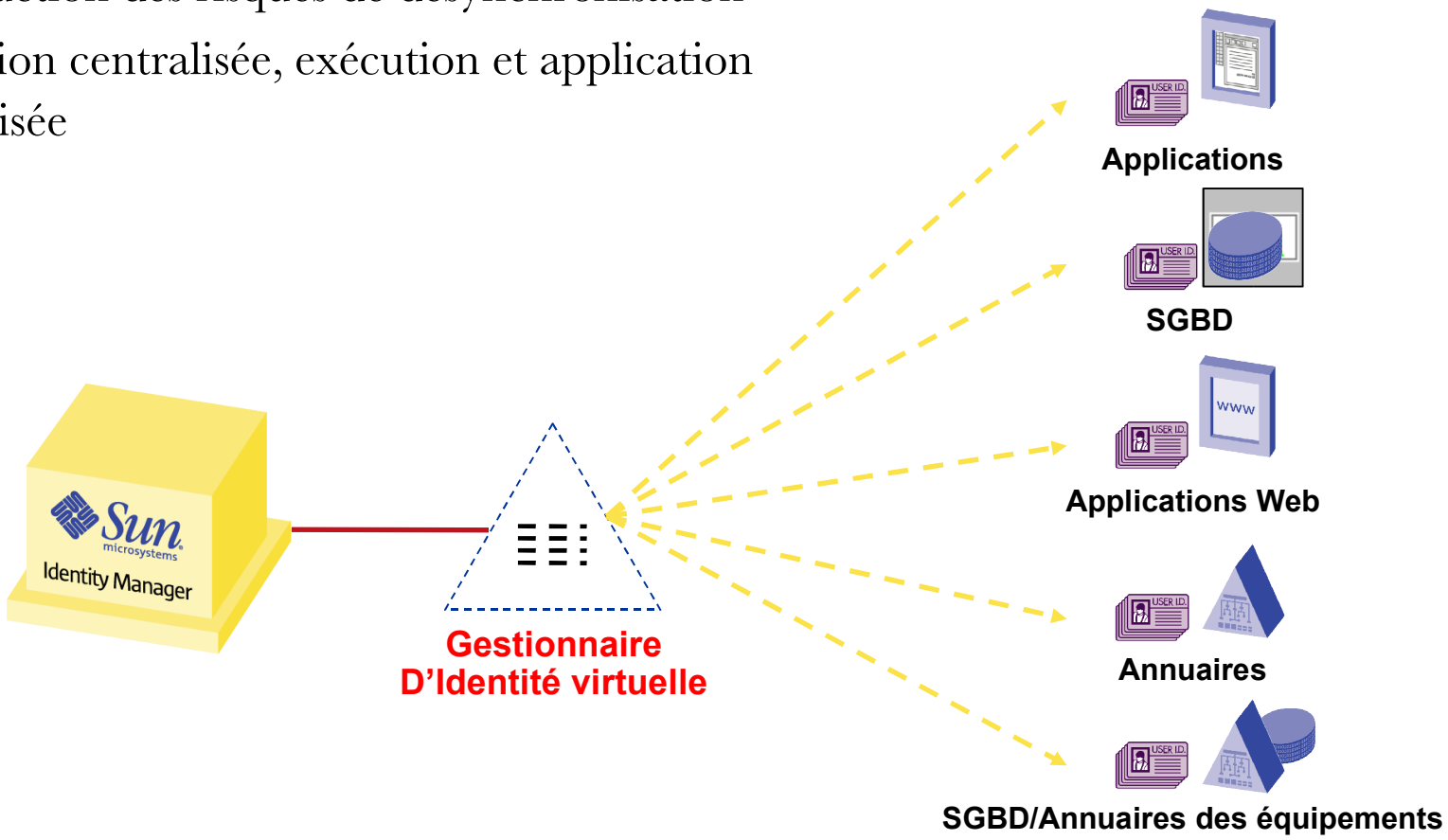


# Apports

Réduction de la durée de propagation

Réduction des risques de désynchronisation

Gestion centralisée, exécution et application localisée

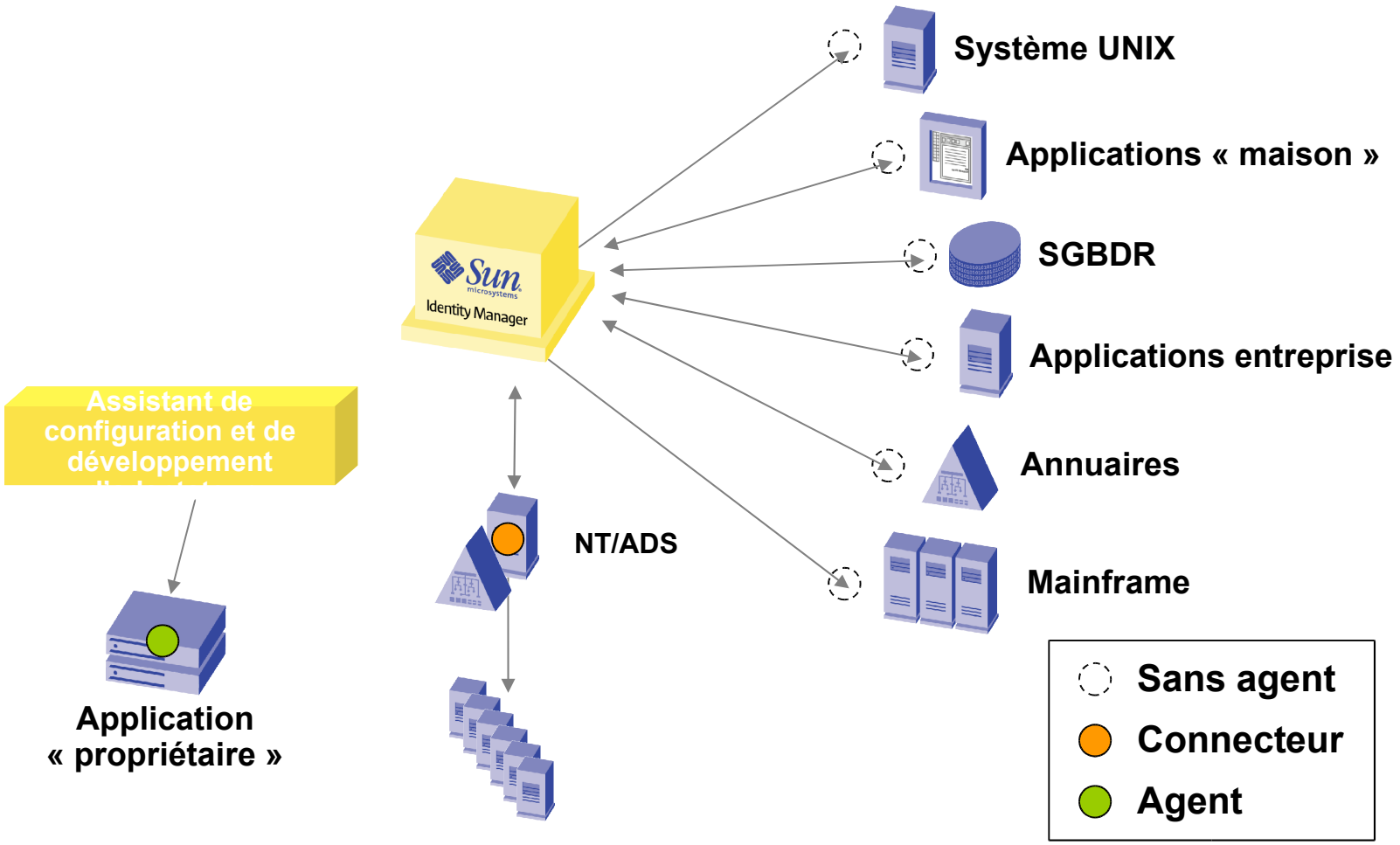


# Connectivité “Sans agents”

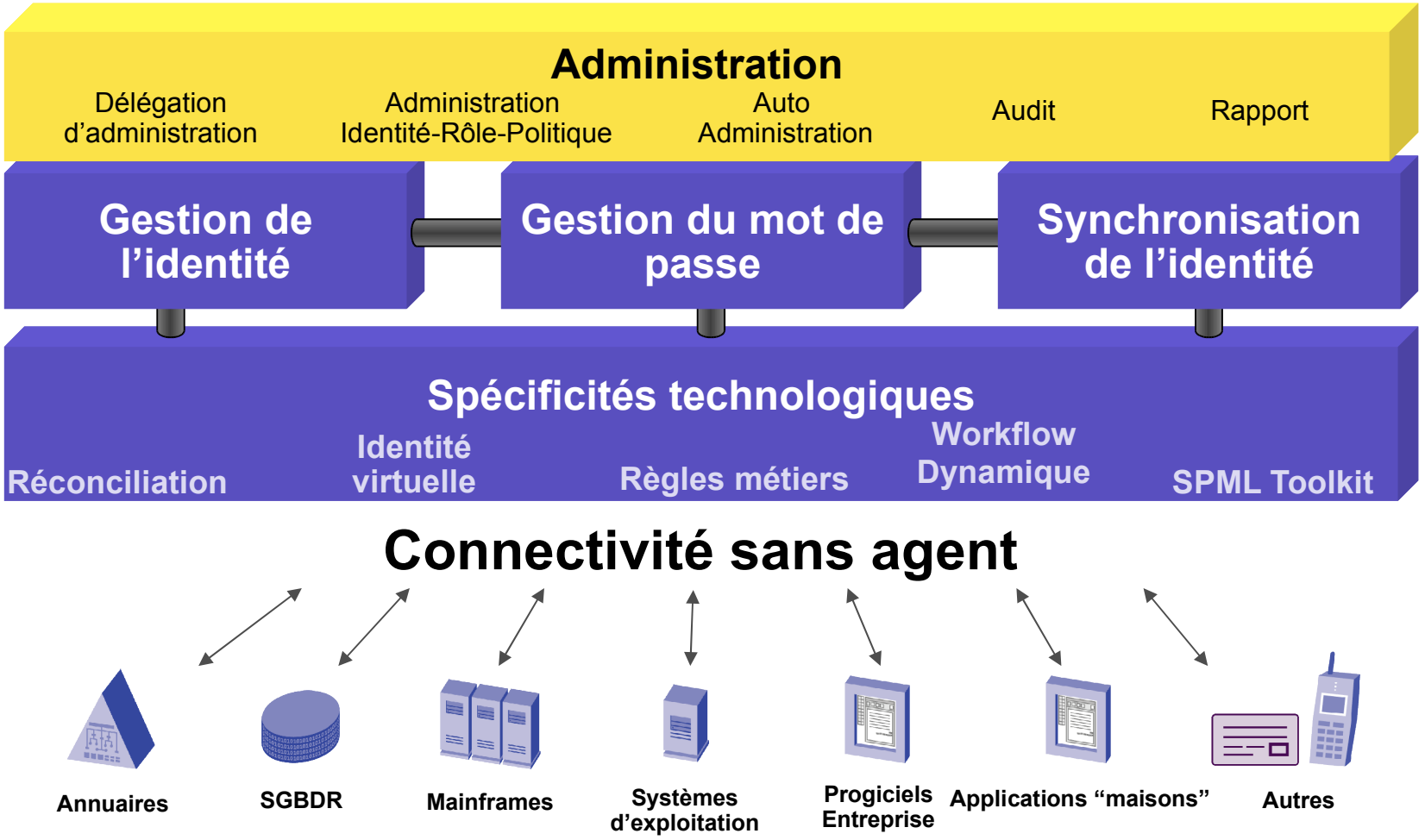
Réduction des contraintes de déploiement

Pas de gestion de la configuration des agents

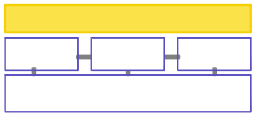
Réduction des contraintes opérationnelles



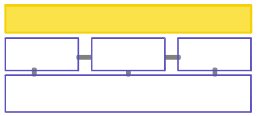
# Sun Java System Identity Manager



# Console de gestion des identités unifiée



# Console de gestion d'identité unifiée



Interface client léger pour les administrateurs gestionnaires et les utilisateurs

- Utilisation des « Smart Forms » : des formulaires web dynamiques et interactifs pour assister l'utilisateur dans sa navigation
- Administration déléguée - granularité élevée : portée, capacités, sources de données, données

Auto-administration : gestion des comptes, du mot de passe, des équipements, des attributs personnels…

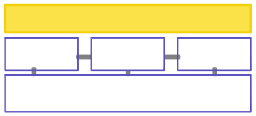
Administrateurs / Gestionnaires

- Définissent et gèrent : les rôles, les politiques, les niveaux de délégation
- Visualisent et gèrent les identités

Génération de rapports détaillés et graphiques

Audit des identités de bout en bout

# Démonstration



# Démonstration

Les différentes interfaces

- Interface d'Administrateur
- Interface de gestionnaire
- Interface Utilisateur

Les Ressources

Les Rôles

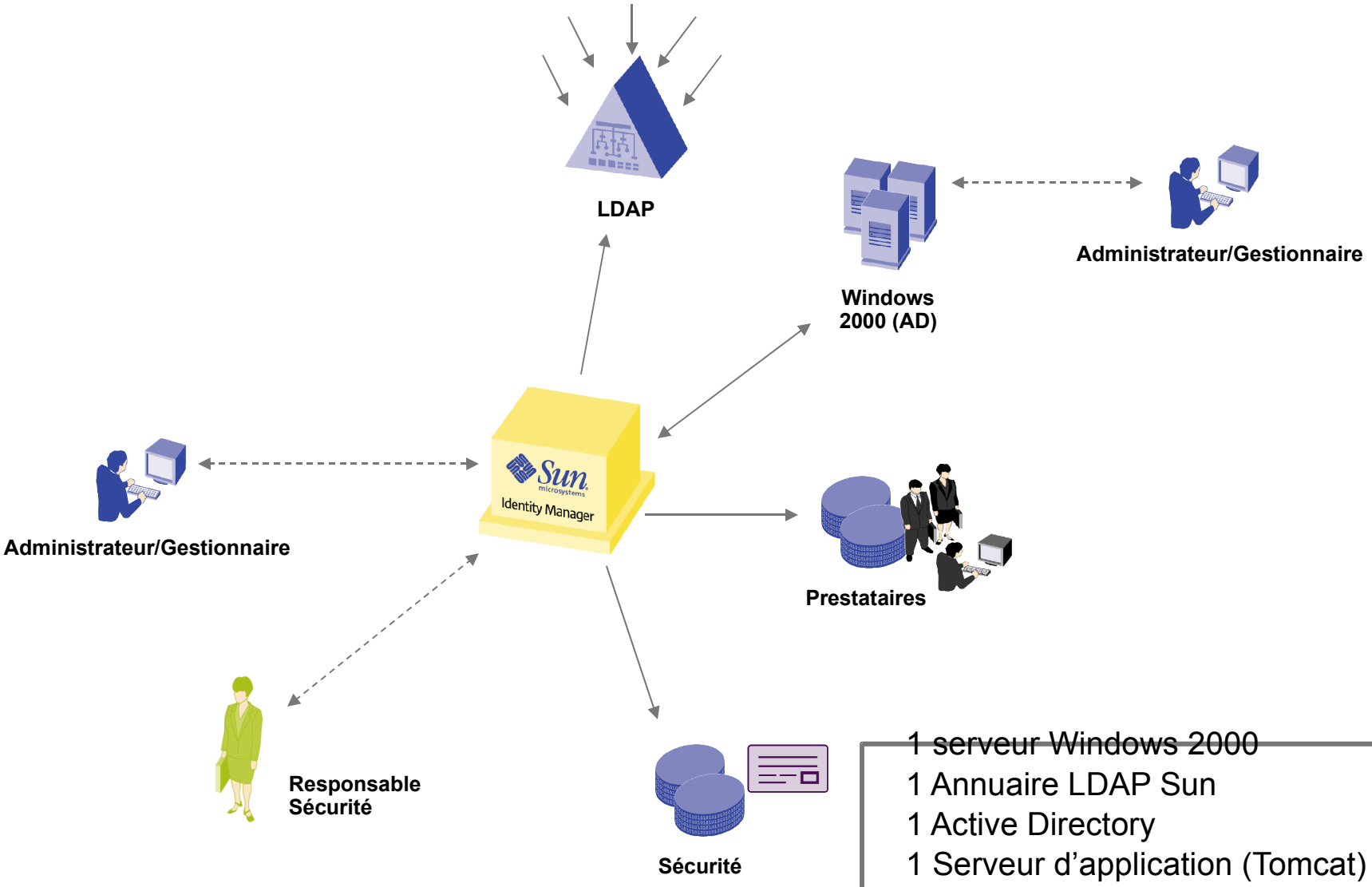
Les Capacités

Les Approbations

La synchronisation

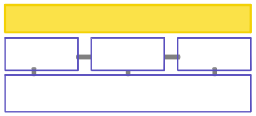
L'auto-administration

# Architecture Logique




1 serveur Windows 2000
1 Annuaire LDAP Sun
1 Active Directory
1 Serveur d'application (Tomcat)
3 bases de données (MySQL)
1 Identity Manager V5

# Démo

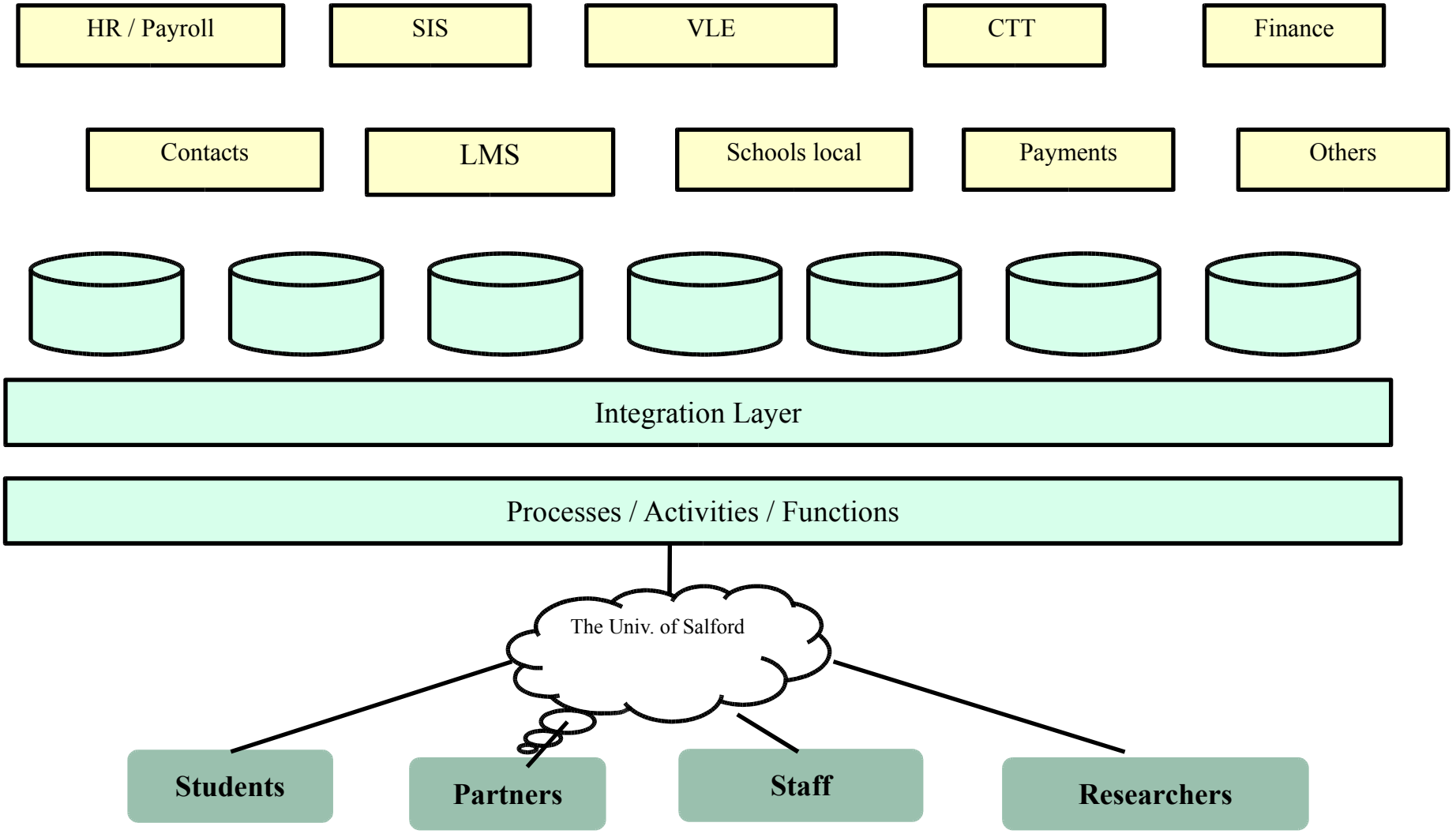


# De la théorie à la pratique

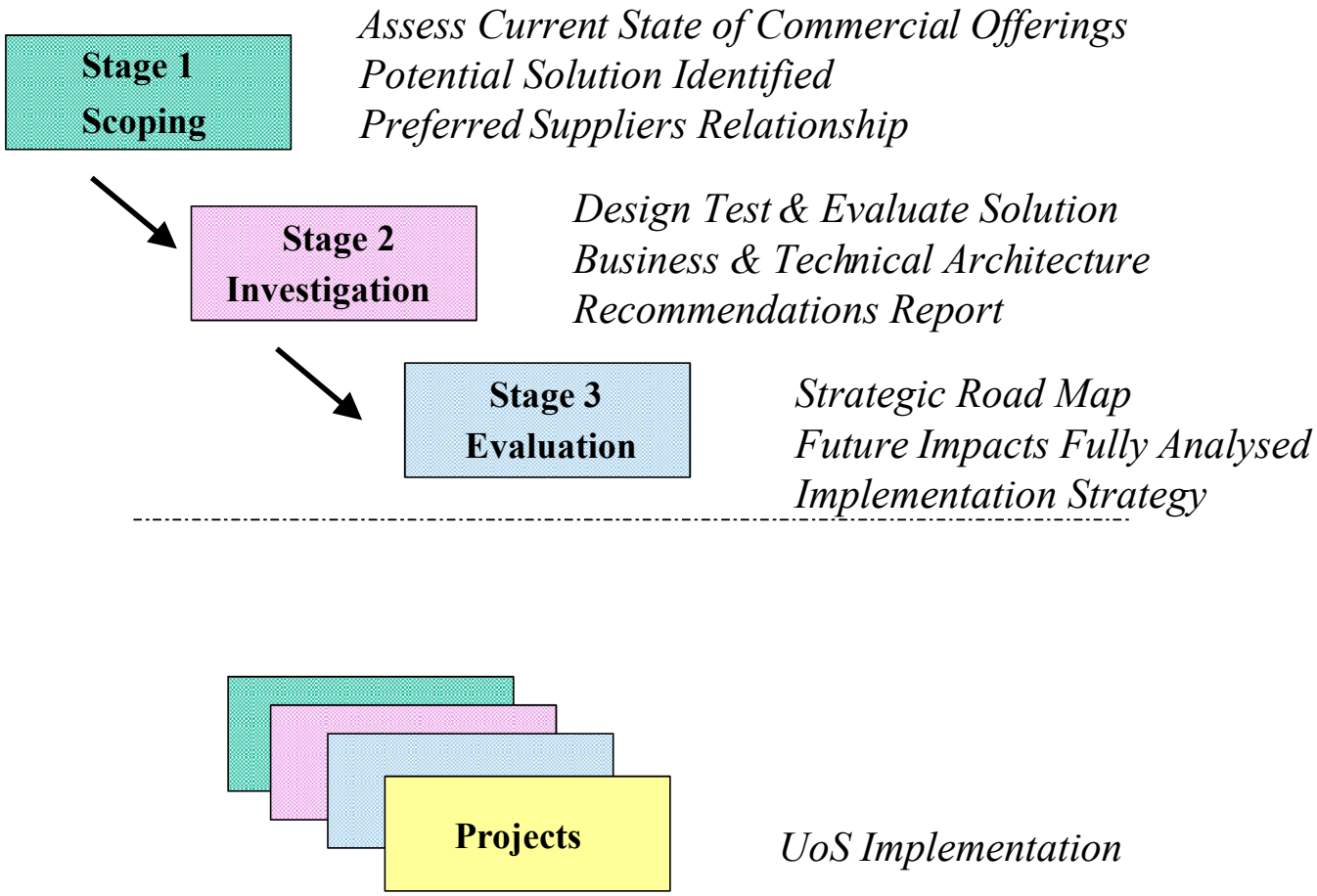
University of Salford
A Greater Manchester University

# Building the Digital Campus
# University of Salford
# February 2005

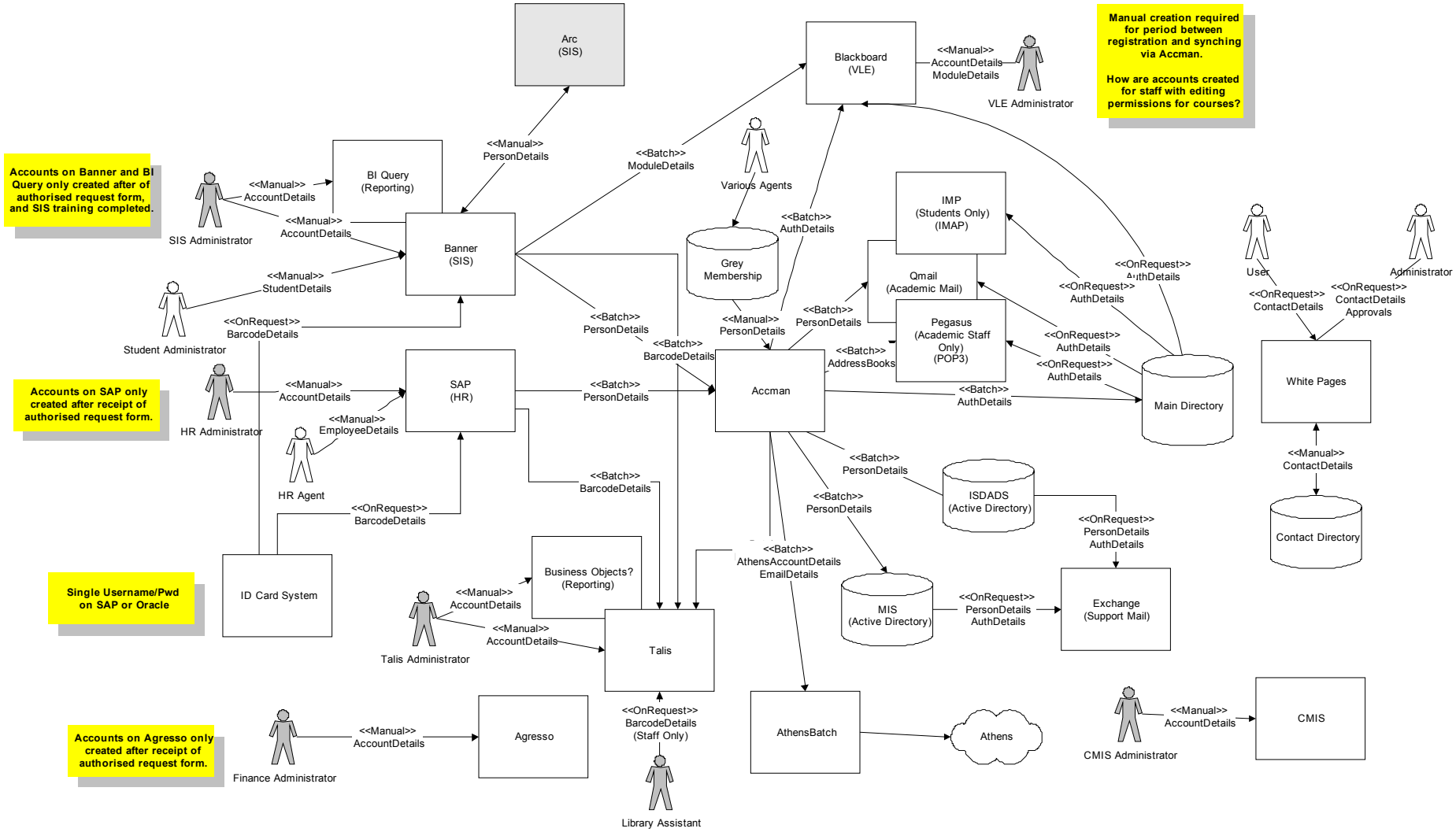
# The Vision: the Integrated Information Infrastructure



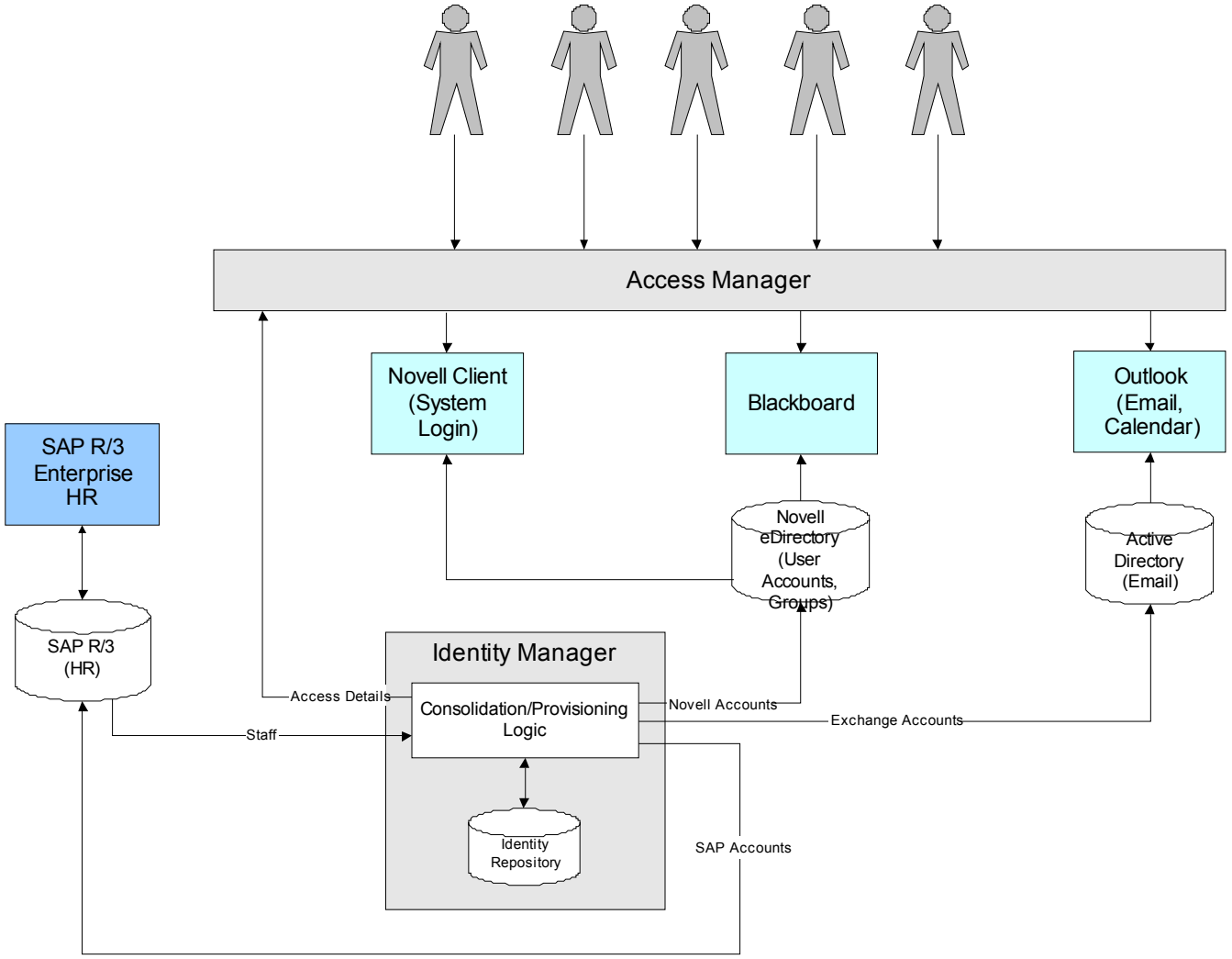
# Proof of Concept Methodology



# Technical Scope – Live



# Technical Scope – Demonstrated



# Identified Business Benefits of IdM

- Greater Flexibility & Control / Improved Efficiency
- Allows for Organisational Changes
- Improved Support Efficiency and Increased Customer Satisfaction
- Streamlining Processes Across the Organization
- Cost Benefits

# Cost Benefits

- Reduced user creation time (through automation)
- Single log-on for users
- Improved security and control (audit trail)
- Reduced and improved working practices (simplified processes)
- Improved integration and business agility (faster change implementation)
- Reduction of Helpdesk activities (reset passwords) and error handling (less manual intervention)
- Enhanced IT service / image to potential customers

# ROI Examples

- Actual Password Reset costs for **Novell only**:
  - Average cost per password reset: **£1.04**
  - Average number of resets per system / year: **3,960**
  - With 10 systems at UoS, average cost of password resets/year: **£41,184**

# Contact

**Martine Carassik**
**Head of Application Development**
**University of Salford**
**m.carassik@salford.ac.uk**

# Identity Management at UC Merced

UC Merced
UNIVERSITY OF CALIFORNIA, MERCED

- Identity solution requirements:
  - Assign a single UCMNetID to each person
  - Eliminate multiple directories (and maintenance)
  - Automatically provision & allow use of appropriate services
  - Adjust or remove access as roles change
  - Provide mappings between systems

- The solution:
  - Directory Server
  - Identity Manager Provisioning Module
  - Identity Manager Meta Directory Module
  - Identity Manager Password Management Module
  - Resource adapters for LDAP, Oracle and Active Directory

# Vers un model Fédéré

# Federation Requirements

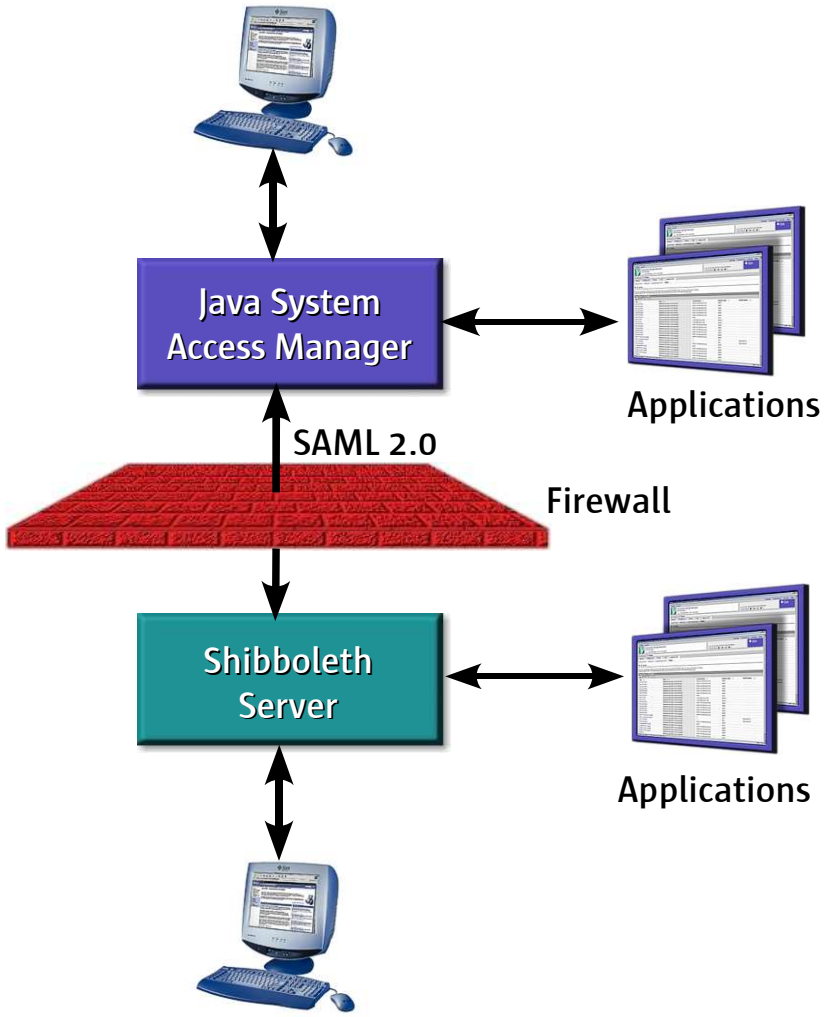
## Federation Enables Sharing Identity Information Outside the Firewall While Protecting Privacy

- Federation is necessitated by collaborative research and other inter-institution collaboration
- There are 2 implementation approaches:
  - **The Liberty Alliance Project** – An alliance of more than 150 companies, non-profit and government organizations developing an open standard for federated network identity (http://www.projectliberty.org/)
  - **Shibboleth** – An open source implementation of federated identity information that has gained a lot of momentum in education
- Shibboleth and Liberty are working on interoperability through SAML 2.0, expected in 12-15 months

# Federation in Java System Access Manager

## Standards-based Approach Allows Integration With Shibboleth

- Supports Federation using Liberty specification
- Interoperability with Shibboleth through SAML 2.0
  (expected in 12-15 months)



# La gestion d'identités: une nécessité sur les campus Numérique

Sun microsystems