Dossier technique

GESTION DES IDENTITÉS

Juillet 2007

Groupe « Gestion des identités »

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS
Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Table des matières

Table des tableaux

Table des figures

LE CLUSIF

Le CLUSIF offre, depuis 1984, un espace d'échanges dans lequel les acteurs de la sécurité des Systèmes d'Information peuvent se rencontrer, travailler et progresser ensemble. A ce jour, le CLUSIF rassemble plus de 600 membres, appartenant à 300 organismes ou sociétés. Sa particularité est d'accueillir les utilisateurs comme les offreurs. De cette complémentarité naît une synergie.

Sa mission

Échanger

La vocation du CLUSIF est de favoriser le partage des expériences.
Les utilisateurs sont ainsi tenus au courant des nouveautés en matière de sécurité et les offreurs ont accès à une meilleure connaissance des besoins et du marché.

Concevoir

La réalisation de travaux sur la sécurité couvre des domaines très étendus, tels que :

- l'état de l'art sur des solutions existantes, des méthodes d'analyse de risques, de conception et de développement sécurisés de projets, d'évaluation de la sécurité des Systèmes d'Information,
- des prises de position sur des sujets d'actualité,
- des enquêtes, des statistiques,
- des guides et des recommandations à caractère didactique.

Promouvoir

Il entre dans les finalités du CLUSIF de sensibiliser et d'influencer un certain nombre d'acteurs de la vie économique et politique, avec le double objectif de promouvoir la sécurité et de faire valoir les besoins et contraintes des utilisateurs auprès des instances dirigeantes. Le CLUSIF s'adresse aux décideurs, utilisateurs, parlementaires, pouvoirs publics, médias, ainsi qu'à d'autres associations.

Éduquer

Le CLUSIF s'implique activement dans le processus d'éducation et de sensibilisation, en matière de sécurité, auprès de ses membres, des professionnels de la sécurité, des enseignants et des étudiants. Il intervient dans les programmes de formation afin que la sécurité des Systèmes d'Information soit incorporée dans les programmes pédagogiques.

Son fonctionnement

Le fonctionnement du CLUSIF repose principalement sur les commissions et les groupes de travail.
Les commissions, à caractère pérenne, sont au cœur de l'activité.
Les groupes de travail, à vocation temporaire, sont créés pour apporter une réponse à des sujets d'actualité ou aux préoccupations d'utilisateurs et d'offreurs. La contribution peut prendre la forme d'un document, d'une recommandation ou d'une prise de position sur un thème donné.

Son réseau relationnel

Régional

Le CLUSIF dispose de relais dans les régions : les Clubs de la Sécurité des Systèmes d'Information Régionaux (CLUSIR). Ces associations indépendantes sont agréées par le CLUSIF et s'engagent à respecter le règlement intérieur et le code d'éthique du CLUSIF. Il existe à ce jour six CLUSIR : Est, Languedoc–Roussillon, Midi–Pyrénées, Nord–Pas de Calais–Picardie, Provence–Alpes–Côte d'Azur, Rhône–Alpes.

International

Le CLUSIF entretient des contacts avec des organismes et des associations en Allemagne, Argentine, Belgique, Canada, Italie, Luxembourg, Maroc, Suisse, Tunisie.

Associatif

Le CLUSIF entretient des relations avec des organismes qui partagent la même sensibilité sur des thèmes de la Sécurité Informatique. Les principaux sont :
AFAI (Association Française d'Audit et du conseil en Informatique)
AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise)
CIGREF (Club Informatique des Grandes Entreprises Françaises)

Institutionnel

Des liens très étroits sont développés avec les pouvoirs publics afin de promouvoir la sécurité des Systèmes d'Information. Le CLUSIF participe ainsi à des groupes de travail internationaux sur la cybercriminalité.

Contact

Secrétariat du CLUSIF
30, rue Pierre Sémard
75009 PARIS
Tel : 01 53 25 08 80 - Fax : 01 53 25 08 88
Courrier électronique : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Audrey	**BALAT**	*CONIX*
Robert	**BERGERON**	*CAPGEMINI*
Annie	**BUTEL**	*BNP PARIBAS*
Myriam	**COTTREAU**	*EURONEXT PARIS SA*
Frank	**DEPIERRE**	*DENY ALL – ASPHANET SA*
Guy	**KHOUBERMAN**	*ACOSS CNIR-SUD*
Lionel	**MOURER**	*BULL SAS*
Witold	**POLOCZANSKI**	*CAPGEMINI*

1 - Introduction

La gestion des identités et des droits d'accès (souvent connu sous l'acronyme IAM, pour Identity and Access Management) est un maillon clé dans la chaîne de sécurité des organisations. Elle permet de renforcer le niveau de sécurité général en garantissant la cohérence dans l'attribution des droits d'accès aux ressources hétérogènes du système d'information.
La gestion des identités et des droits d'accès est également devenue l'un des moyens majeurs permettant de répondre aux exigences réglementaires de plus en plus fréquentes concernant la traçabilité. C'est aussi un moyen d'optimiser l'administration des droits.

Mais qu'entend-on exactement par gestion des identités et des droits d'accès ?

La gestion des identités consiste à gérer le cycle de vie des personnes (embauche, promotion, mutation, départ, etc.) au sein de la société et les impacts induits sur le système d'information (création de Comptes utilisateurs, attribution de Profils utilisateurs, mise en œuvre du contrôle d'accès, etc.). Cette gestion des identités doit pouvoir être faite d'un point de vue fonctionnel par des non-informaticiens (exemple : Ressources Humaines, Maîtrise d'ouvrage, l'utilisateur lui-même) et d'un point de vue technique par des informaticiens (exemple : administrateur, Maîtrise d'œuvre). La solution de gestion d'identités doit être une solution globale sur la base d'une infrastructure centralisée avec une gestion fonctionnelle distribuée et qui intègre les fonctionnalités suivantes :

- la gestion du référentiel central des utilisateurs (alimentation à partir de référentiels utilisateurs sources),
- la gestion du référentiel central des ressources concernées par la gestion des droits d'accès,
- la gestion des habilitations (gestion des Profils, Rôles, gestion des utilisateurs, workflow),
- le provisioning (synchronisation des référentiels cibles de sécurité),
- l'administration décentralisée,
- l'auto-administration, gestion par les utilisateurs des mots de passe et des données privées,
- l'audit et le reporting,
- le contrôle d'accès (authentification, autorisation).

Ce document vous permettra de vous familiariser avec les concepts et la modélisation utilisés dans une démarche de gestion des identités. Il a également pour but de vous aider à mener à bien un projet de gestion des identités et vous guider dans vos choix d'architecture.

2 - État des lieux

Aujourd'hui, la multiplication et la diversité de systèmes de contrôle d'accès liés aux systèmes d'exploitation et aux applications est devenue particulièrement contre-productive. En effet, chaque « système » (OS, NOS, messagerie, groupware, applications métiers, ERP, CRM, etc.) est protégé par une procédure de contrôle d'accès spécifique. De fait, chaque fonction à réaliser peut nécessiter un code d'accès et des droits associés. Cette multiplicité de contrôles d'accès est source de confusion pour l'utilisateur qui, par exemple, perd ou oublie ses mots de passe. Il lui reste alors deux solutions : soit il sollicite le service de help-desk, au risque de l'engorger en lui faisant perdre trop de temps à réinitialiser très souvent des mots de passe, soit il note lesdits codes sur un support à sa portée pour ne plus les oublier ! Bien entendu, aucune de ces solutions n'est satisfaisante…

D'une manière générale, chaque système d'exploitation et/ou application est géré par un administrateur unique ; de fait, toute vision globale est impossible. Dans ce cas, l'administration autonome de chaque système est particulièrement source d'erreurs, de vulnérabilités et de perte de temps. Par exemple, ne pas avoir la vision globale sur les droits de l'ensemble des utilisateurs peut engendrer des problèmes de responsabilité (devenus importants dans le cadre des nouvelles lois ou réglementations), tel qu'un acheteur qui validerait sa propre commande.

Généralement, les nouveaux arrivants[1] se voient attribuer plus ou moins rapidement certaines ressources (un bureau, un téléphone, un badge d'accès, un PC, etc.), mais ne peuvent pas travailler, faute de droits d'accès. Ceci est notamment du au fait que le délai d'attribution des ressources et des droits est trop long, que les circuits d'attribution sont trop « lourds », etc. Ils doivent même souvent se débrouiller seuls : trouver le bon responsable pour l'accès à telle base de données, à telle application, à l'Intranet, etc. La liste des interlocuteurs est à la mesure de la complexité du Système d'Information.

D'autre part, on est rarement certain d'avoir supprimé tous les droits dont disposait un employé partant ou d'avoir mis à jour les droits d'un employé en cas de changement de fonction. Le Système d'Information regorge souvent de comptes dits « fantômes » (dormants et/ou périmés).

De plus, les comptes techniques génériques, installés par défaut, par les systèmes d'exploitation et/ou les applications, ne sont pas toujours modifiés, voire supprimés, induisant d'autres failles. Ceci étant d'autant plus grave que ces mots de passe sont facilement accessibles sur Internet… De même, certaines personnes utilisent, lorsqu'elles arrivent dans l'entreprise, des comptes utilisateurs « génériques » et partagés, simplement du fait de la durée importante de création de leur propre compte.

Enfin, l'audit et la traçabilité sont souvent les parents pauvres de la mise en œuvre des droits d'accès des utilisateurs. Pourtant, de plus en plus, les entreprises doivent respecter des normes, des lois et/ou des réglementations strictes en matière de politique de contrôle interne.

[1] Il s'agit ici d'un employé de l'entreprise. Mais n'oublions pas qu'avec l'ouverture du Système d'Information, l'entreprise donne aussi de plus en plus accès à ses clients, ses fournisseurs voire ses partenaires commerciaux.

Illustration

Si nous prenons l'exemple du référencement d'un nouvel utilisateur dans un Système d'Information, nous pouvons identifier les actions suivantes :

- embauche dans une entreprise ⇨ Référencement dans le système de gestion de la paie,
- attribution d'un bureau ⇨ Référencement dans la base du service logistique,
- attribution d'un numéro de téléphone ⇨ Référencement dans la base téléphonique,
- attribution d'un ordinateur, d'un identifiant et d'un mot de passe pour accéder au réseau ⇨ Référencement dans le système bureautique,
- attribution d'un badge pour l'accès aux locaux ⇨ Référencement dans le système de gestion des badges,
- droits d'accès à un restaurant d'entreprise ⇨ Référencement dans la base du restaurant d'entreprise,
- droits d'accès sur une application ⇨ Référencement dans la base de l'application,
- etc.

Dans la majorité des entreprises, ces opérations font appel à des annuaires qui ne sont ni compatibles entre eux, ni synchronisés (cf. Figure 1 ci-dessous). Ainsi pour un nouvel utilisateur il faut saisir plusieurs fois les mêmes informations dans des systèmes différents par des personnes différentes et il en va de même en cas de modification d'une information. Cette mise à jour est parfois très longue ou que partiellement réalisée.

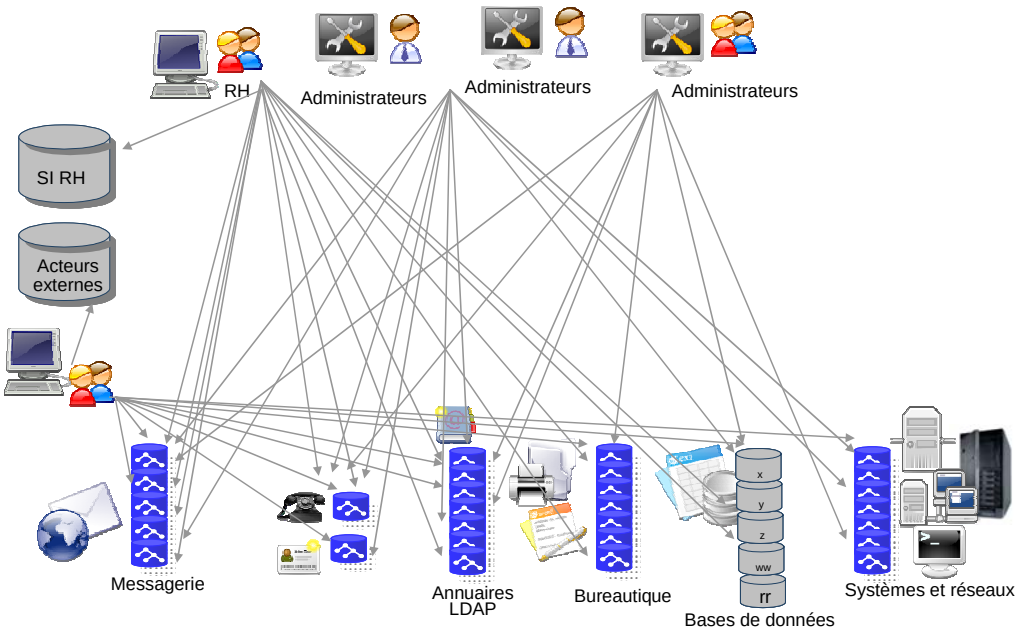

Figure 1 – Existant « standard » de la gestion des identités et des droits d'accès

3 - Justifications d'un projet de gestion des identités et des droits d'accès

Comme nous l'avons vu au chapitre précédent, l'absence de gestion globale des identités et des droits d'accès peut générer de nombreux problèmes, parmi lesquels :

- la perte de productivité due aux délais d'obtention des droits d'accès,
- une charge importante d'administration (multiplication des administrateurs, réinitialisation des mots de passe, etc.),
- l'impossibilité de tracer les actions d'administration des droits et d'en contrôler la cohérence et la pertinence,
- la difficulté d'auditer les accès aux ressources,
- des entorses au principe de séparation des tâches,
- le non respect des contraintes légales et/ou réglementaires (par exemple au travers d'un mauvais paramétrage des règles de gestion).

La justification d'un projet de gestion des identités et des droits d'accès reposera sur les améliorations suivantes :

- garantie de traçabilité et d'auditabilité afin de répondre aux obligations légales et/ou réglementaires,
- repositionnement des « propriétaires fonctionnels » au centre du débat,
- réduction des coûts d'administration,
- amélioration de l'efficacité et de la réactivité,
- amélioration de la sécurité (adéquation des droits aux besoins métier).

L'ensemble des flux présentés dans le chapitre précédent va pouvoir être représenté de la manière suivante après la mise en place d'une gestion centralisée des identités (cf. Figure 2).

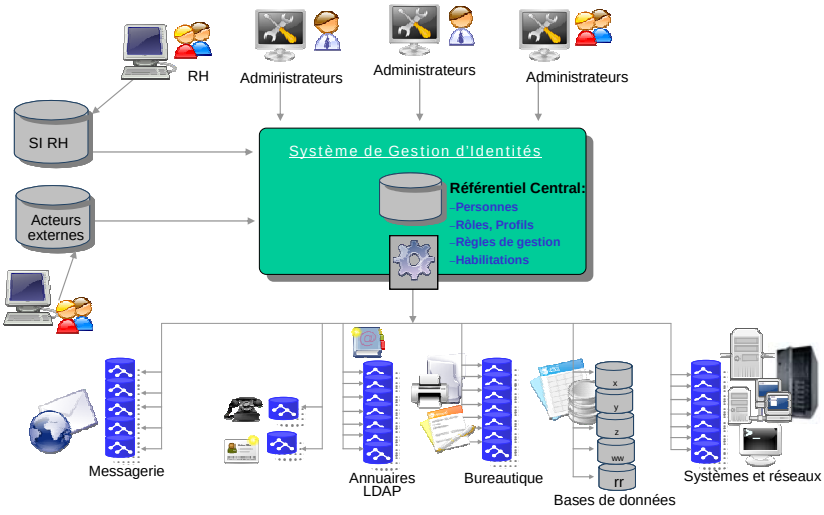

Figure 2 – Flux de mise à jour après la mise en place d'une gestion centralisée

Les informations sont mises à jour dans le référentiel central qui alimente ensuite automatiquement les annuaires ou bases de sécurité des différents environnements.

3.1. Garantie de traçabilité et d'auditabilité

Les principales lois et réglementations impliquant le SI et ayant des impacts directs sur les aspects traitant de la sécurité (en particulier traçabilité et auditabilité) sont présentées dans le chapitre 7 – « aspects juridiques ».

D'une manière générale, ces lois et règlements « imposent » au Système d'Information des exigences de :

- continuité d'activité,
- de séparation des tâches : par exemple, une même personne ne doit pas à la fois commander une fourniture ou prestation et valider sa réception,
- de traçabilité et d'auditabilité : permettant de valider « qui a fait quoi » au sein du système d'information, et « qui a habilité qui »,
- de respect de la vie privée.

Déroger à ces exigences peut entraîner un risque juridique pour les responsables de l'entreprise.

3.2. Réduction des coûts d'administration

Un système de gestion des identités et des droits d'accès permet d'alléger la charge de travail de l'équipe de « support informatique » (administration, help desk). Cet allègement résulte d'une part de l'automatisation de tâches de gestion de comptes (réduction du nombre d'administrateurs) et d'autre part de la diminution du nombre d'appels d'utilisateurs (perte ou oubli de nombreux mots de passe, relance de demandes d'accès, etc .).

Le système de gestion des identités peut permettre aux utilisateurs la gestion directe de certains aspects de leur profil (par exemple le mot de passe, l'adresse, les numéros de téléphone, etc.).

3.3. Amélioration de l'efficacité et de la réactivité

Un système de gestion des identités et des droits d'accès permet de réduire le nombre d'interventions humaines par une automatisation de la propagation des droits sur les différents environnements concernés. La conséquence est à la fois une réduction des délais de mise à disposition des droits d'accès et une réduction des sources d'erreur (prise en compte systématique de tous les besoins liés à l'activité de l'utilisateur, garantie de cohérence dans les droits attribués).

Les gains générés concernent à la fois les utilisateurs internes (gain de productivité) et externes (amélioration de la qualité du service et de l'image de l'entreprise).

Sur un autre plan, lors d'une fusion ou d'une acquisition, il faut fournir le plus rapidement possible un accès aisé aux ressources rassemblées d'entreprises auparavant autonomes. Là encore, une solution de gestion des identités et des droits d'accès aidera à relever ce défi au

travers d'un service d'intégration des informations multi-plates-formes permettant de connecter les systèmes de chaque entreprise à la plupart des systèmes (nouveaux ou préexistants) de la nouvelle entité.

3.4. Amélioration de la sécurité

Un système de gestion des identités et des droits d'accès permet de renforcer la sécurité. Une telle approche conduit à établir des liens entre toutes les applications, bases de données et annuaires en s'appuyant sur des notions de rôle et de profil. Cette solution offre un point unique de gestion des règles de sécurité pour l'ensemble des systèmes concernés. Elle permet de créer simplement des règles d'accès et de sécurité, en cohérence avec la Politique de Sécurité des Systèmes d'Information et les besoins métier, puis de les propager automatiquement à tous les systèmes de l'entreprise.

La gestion centralisée des identités permet d'éliminer une source considérable d'erreurs d'administration pouvant causer des failles de sécurité d'accès au SI de l'entreprise. Elle permet également de résilier complètement et immédiatement les droits d'accès sur l'ensemble des systèmes lorsque des salariés ou personnels extérieurs quittent l'entreprise ou changent d'affectation et supprimer ainsi les comptes « fantômes ».

En mettant en place des processus maîtrisés d'habilitation, le système permet d'impliquer les responsables métiers dans le circuit d'habilitation et de ne plus laisser au seul administrateur technique la maîtrise des droits d'accès.

4 - Concepts et modélisation

4.1. Les concepts

Ce chapitre introduit les concepts et les objets manipulés, avant de décrire les mécanismes de gestion des identités et des habilitations.
En présence de nombreux modèles théoriques, et en l'absence de normalisation, la terminologie utilisée dans ce chapitre est issue de retours d'expérience.

4.1.1 Personne (utilisateur / acteur)

Désigne une personne physique : les employés d'entreprise, les prestataires, les partenaires et les clients de l'entreprise qui, de par leur fonction, exercent une activité ayant vocation à leur permettre de bénéficier des applications et des ressources mises à disposition par l'entreprise.

Toute personne déclarée dans un référentiel central de sécurité et de gestion des habilitations est identifiée par un identifiant unique.

Des attributs supplémentaires fournissent les informations concernant la personne. Ces attributs sont :

- un nom,
- un prénom,
- une durée de validité,
- un état (actif, suspendu),
- les périmètres d'accès autorisés,
- un niveau de confidentialité (par domaine d'activité),
- etc.

Tout acteur du système est déclaré d'une manière unique dans un référentiel central de sécurité et de gestion des habilitations en tant que personne physique et peut disposer de comptes dans différents environnements et applications en fonction des habilitations accordées.

La cohérence de ces informations est maintenue automatiquement par le système de gestion des habilitations.

D'une manière générale les autorisations ne sont pas attribuées directement aux personnes mais à travers des profils/rôles. Certaines autorisations particulières peuvent être associées à la personne physique. Elles sont limitées aux autorisations d'accès global au SI d'entreprise comme limitation temporelle ou géographique d'ouverture de session ou suspension générale d'accès.

4.1.2 Compte 

À chaque personne peuvent être associés des comptes d'accès aux différents systèmes et applications.
Le compte est défini par l'identifiant d'accès, un mot de passe (ou un authentifiant d'une autre nature), et plusieurs attributs supplémentaires en fonction de l'environnement dans lequel il est crée comme : la politique de mot de passe associée, l'accès externe autorisé ou non, l'état du compte, les modes d'authentification autorisés etc.

Il existe quatre types de comptes :

- le **compte global**. Ce compte, unique (à un utilisateur correspond un seul compte) identifie une personne dans le référentiel central de gestion des habilitations et est utilisé par tous les processus d'attribution des droits,
- le **compte utilisateur**. Ce compte donne l'accès à un utilisateur dans un environnement particulier auquel cet utilisateur est habilité. Chaque compte utilisateur est obligatoirement associé à une personne (et son identifiant unique). Sa création / suppression et la cohérence des informations associées est maintenue automatiquement par le système de gestion des habilitations en fonction des profils métiers attribués à la personne. Exemples : compte d'OS, de NOS, de messagerie, de groupware, de LDAP, etc. Les administrateurs locaux peuvent créer des comptes utilisateur uniquement dans les cas exceptionnels (exemples : audit de plateforme, intervention technique d'urgence, …). Une procédure de « réconciliation » doit être appliquée ensuite pour définir les liens entre ce compte et la personne.
- le **compte d'administration**. Ce compte donne l'accès à un administrateur dans un environnement particulier. Ce compte n'est pas associé à une personne. Il ne correspond donc à aucune entrée dans le référentiel central. ***Leur usage doit être limité aux actes d'administration techniques des environnements et des applications dans les environnements où ces tâches ne peuvent pas être effectuées via les rôles d'administration***. Exemple : Compte « Root » d'Unix. Les procédures mises en œuvre doivent garantir la traçabilité et l'auditabilité des personnes physiques auxquelles ces comptes administrateurs ont été autorisés d'emploi. Un changement d'affectation doit être associé à une procédure de changement des mots de passe.
- le **compte « de service fonctionnel ou technique »**. Ces comptes sont utilisés par les composants d'un système pour accéder aux services applicatifs et/ou données d'un autre système. La connexion au système cible, utilisant ce compte, doit être authentifiée ou seulement identifiée si la liaison se fait intégralement dans une zone sécurisée. Le compte est donc associé au système ou application cliente et non à une personne. Aucune personne n'est autorisée à l'utiliser. Les permissions sont définies et gérées dans le cadre d'administration d'application et ne sont pas prises en charge par le système de gestion des habilitations. Les droits attribués à ce compte doivent être restreints au strict minimum et n'autoriser que les fonctions invoquées. Le système de nommage adopté devrait différencier clairement ce type de comptes.

Un compte (unique dans un environnement) est associé à une et une seule personne à l'instant T *(à l'exception des comptes d'administration et techniques).*

À un compte peuvent être associés (en fonction de la capacité de gestion de l'environnement) :

- une durée de validité,
- un état (actif, suspendu),
- etc.

4.1.3 Rôle 

Un rôle définit les permissions nécessaires à l'utilisation des objets (applications et/ou des ressources).

Le rôle applicatif est un ensemble de droits propres à une seule fonction dans une application. Par exemple : le droit d'usage d'un jeu d'écrans et de menus correspondant à une fonction dans l'application.

Une habilitation donne à un utilisateur un ensemble de permissions dans une application. Elle est attribuée en fonction du poste opérationnel au sein de l'organisation et non à titre individuel. C'est le poste opérationnel qui détermine les rôles et les périmètres nécessaires.

L'habilitation est affectée à la personne via l'attribution des rôles applicatifs :

- un rôle applicatif appartient à une seule application.
- l'application admet plusieurs rôles.
- un rôle ne peut pas être affecté directement à l'utilisateur mais uniquement par l'intermédiaire d'un profil métier.
- sont associés au concept de rôle :
    - les modes d'authentification autorisés,
    - les périmètres d'accès autorisés,
    - la cardinalité (nombre d'occupants maximum autorisés),
    - la séparation statique des pouvoirs (rôles interdits de cohabitation).

4.1.4 Profil 

Pour faciliter la gestion des habilitations, il est courant de lier l'attribution d'un ensemble d'habilitations à l'obtention d'un profil « fonctionnel ».

Un profil fonctionnel regroupe un ensemble de rôles nécessaires à l'exécution d'une fonction métier. Ce profil peut également être vu comme un package de rôles applicatifs ou un niveau supérieur dans la hiérarchie des rôles (Cf. modèle RBAC hiérarchique § 4.2.2).
Un utilisateur peut avoir un ou plusieurs profils fonctionnels.

Le profil d'habilitation, auquel sont rattachés, via les rôles, les droits d'accès aux applications, est déterminé par le poste opérationnel (Cf. § 4.1.5). A chaque poste est associé un ou plusieurs profils d'habilitation.

Le profil correspond généralement à la fonction exercée par l'acteur affecté au poste opérationnel ainsi qu'à son niveau d'expertise. Il peut aussi correspondre à un ensemble d'habilitations spécifiques.

Dans le but d'optimisation de gestion des profils, on pourra ajouter des profils utilisateurs dits de « factorisation » :

- profil « général » : décrit l'accès standard messagerie, pages jaunes, pages blanches, etc,
- profil « métier » : décrit l'ensemble des services accédés en standard par une personne appartenant à un métier de l'entreprise.

Ainsi, une personne pourra être associée à plusieurs profils utilisateur : profil général, profil(s) métier(s).

4.1.5 Le poste opérationnel

Le poste opérationnel (position de travail) correspond à une fonction métier exercée au sein d'un élément de structure (service, département, …). Un poste opérationnel est toujours défini au sein d'un et un seul élément de structure. Le responsable de structure indique les postes qui lui sont attribués.

Un poste peut éventuellement être partagé par plusieurs acteurs.

Le poste opérationnel n'est pas modélisé dans le référentiel central.

4.1.6 Groupe 

Les utilisateurs peuvent être regroupés, dans le référentiel central, en groupes statiques ou dynamiques. Ces groupes sont utilisés pour faciliter la gestion en masse des habilitations.

4.1.7 Perimètre

Le périmètre est utilisé par les applications et/ou systèmes pour affiner le contrôle d'autorisation qu'ils réalisent.

Le périmètre peut avoir trois types différents (temporel, géographique et fonctionnel) et être associé à :

- une personne
- un compte (uniquement dans le cas de limitation des autorisations d'accès à des ressources d'un environnement)
- un rôle.

Il ne peut pas être associé à un profil.

4.1.8 Périmètre Temporel 

Le périmètre temporel permet de restreindre les possibilités d'accès d'un utilisateur dans le temps.

Plusieurs types de restrictions sont possibles :

- période :
  - définis par : <Date début – Date fin>,
  - l'accès n'est autorisé que si la date du jour se situe entre les deux dates spécifiées,
- plage horaire :
  - définie par :<Heure début – Heure fin>,
  - l'accès n'est autorisé, chaque jour, que si l'heure (locale du système d'autorisation) se situe entre les heures spécifiées,
- calendrier :
  - défini par <la liste des jours de la semaine>,
  - l'accès n'est autorisé que si le jour de la semaine (local du système d'autorisation) correspond à une des entrées de la liste :
    - <la liste des jours calendaires> (ex : 26/01, 30/06, etc.),
    - <la liste des semaines> (S2, S3, etc.),
    - <la liste des mois (Janvier, Février…) calendaires>.

Ces limitations sont appliquées par les différents systèmes d'autorisation en fonction de la capacité du système à gérer ce type de restriction.

Le périmètre temporel peut être associé à :

- une personne,
- un rôle,
- une ressource.

Un périmètre temporel associé à une personne limite son accès à l'ensemble des ressources et applications en empêchant l'utilisateur d'établir une session en dehors de périodes autorisées.

Un périmètre temporel associé à un rôle limite l'accès à l'application ou à un ensemble de ressources :

- dans le **cas d'une application**, il empêche l'utilisateur d'exécuter l'application (contrôlé par l'application elle-même) en dehors des périodes autorisées. Le profil de l'utilisateur présentera donc un ensemble des applications disponibles variable dans le temps,
- dans le **cas d'une ressource**, il empêche l'utilisateur d'établir une session, dans l'environnement qui héberge les ressources concernées, en dehors des périodes autorisées.

De fait, la limitation temporelle s'applique donc à un compte d'utilisateur dans ces environnements. Cette association doit être gérée par le système de gestion des habilitations (en fonction des limitations des personnes ou des rôles) et transmise aux différents systèmes de contrôle d'accès pour application.

4.1.9 Périmètre Géographique 

Le périmètre géographique permet de restreindre les possibilités d'accès d'un utilisateur en fonction du lieu à partir duquel il accède au SI.

Plusieurs types de restrictions sont possibles :

- **un lieu** : l'accès n'est autorisé que si la session est ouverte à partir du ou des postes situés dans un lieu ou dans un groupe des lieux autorisées,
- **une typologie d'accès** : l'accès n'est autorisé que si la session est ouverte à partir d'une ou des zones réseau autorisées. La typologie d'accès est par exemple :
  - soit un accès à partir du réseau particulier,
  - soit un accès à partir du service d'accès distant,
  - soit un accès distant à partir du réseau partenaire,
- **le poste de travail** : l'accès n'est autorisé que si la session est ouverte à partir du ou des postes autorisés.
  - le poste de travail est un poste 'physique' sur lequel on souhaite autoriser ou interdire certaines opérations afin d'éviter, par exemple, qu'un utilisateur ne puisse intervenir sur certains postes dédiés à des cellules spécialisées.
  - le poste peut être identifié par :
    - n° du terminal (liste des numéros, un sous-ensemble du numéro),
    - n° d'inventaire (gestion du parc) … (liste des numéros, un sous-ensemble du numéro),
    - l'adresse IP (ou le groupe des adresses IP de sous-réseau),
    - etc.

Les limitations géographiques sont appliquées par les différents systèmes d'autorisation en fonction de la capacité du système à gérer ce type de restriction.

Le périmètre géographique peut être associé à :

- une personne,
- un rôle.

Un périmètre géographique associé à une personne limite son accès à l'ensemble de ressources et applications en empêchant l'utilisateur d'établir une session à partir des lieux non autorisés.

Un périmètre géographique associé à un rôle limite l'accès à une application en empêchant l'utilisateur d'exécuter l'application (contrôlé par l'application elle-même) à partir des lieux non autorisés. Le profil de l'utilisateur présentera donc un ensemble des applications disponibles variable en fonction du lieu de présence.

Cette relation permet de dédier certains postes de travail à des opérations spécifiques.

4.1.10 Périmètre Fonctionnel 

On désigne sous ce terme les limitations imposées par le programme de contrôle d'une application. Transmis à l'application lors de l'appel des transactions associées au rôle, il

permet de gérer la sécurité applicative : le programme autorisera ou non certains traitements en fonction des données qui lui seront communiquées par le système d'habilitation (identifiant acteur, poste de travail, éventuellement lieu de présence ou d'affectation d'utilisateur, etc).

Le périmètre fonctionnel peut être associé à :

- un rôle.

Plusieurs types de données servant de base aux restrictions sont possibles :

- mode d'authentification,
- périmètre géographique :
  - poste de travail,
  - lieu de présence lors de la session courante,
  - groupe de lieux de présence lors de la session courante,
  - entité d'attachement administratif,
- degré d'expertise associé au rôle. *Un acteur peut n'exercer aucune activité d'expertise. Il peut éventuellement être expert en plusieurs domaines.*

Cette liste n'est pas exhaustive et peut être enrichie par toute application si nécessaire.

La nature d'information et surtout son interprétation sont gérées exclusivement par l'application.

4.1.11 Mode d'authentification

Certaines applications critiques imposent un mode d'authentification particulier (authentification forte). Le système d'authentification fournit (dans le contexte de sécurité) l'information indiquant le mode d'authentification utilisé lors de l'ouverture de la session. Cette information est exploitée par le système de contrôle d'accès et /ou l'application.

Le mode d'authentification peut être associé à :

- un rôle,
- une ressource.

4.1.12 Ressource

La ressource est définie par :

- un libellé,
- les modes d'authentification nécessaires pour y accéder,
- les périmètres d'accès autorisés,
- les rôles ou les groupes de comptes autorisés sur cette ressource.

Par ailleurs, l'autorisation d'accès du rôle ou des groupes de comptes peut être suspendue à tout moment si besoin.

Une ressource désigne par exemple :

- une ou des adresses IP de serveurs,
- une ou des URL,
- une commande de lancement d'une application,
- etc.

À une ressource peuvent être associés :

- un périmètre temporel (durée de validité),
- un état (actif, suspendu).

Elle est utilisée lors de la connexion des utilisateurs au réseau.

4.1.13 Environnement du SI

Le terme d'environnement du SI désigne un ensemble de ressources et de processus (système, sous-système, application, etc.) dont les droits d'accès sont gérés par un système de contrôle unique et autonome et administré par l'entité responsable.

Exemples :

- les fichiers, répertoires, files d'attente, services de NOS,
- les fichiers, répertoires d'OS,
- les ressources et les services applicatifs,
- les messageries et groupware,
- les bases de données relationnelles,
- etc.

4.1.14 Environnement externe

Le terme d'environnement externe désigne un ensemble de ressources et de processus (système, sous-système, application, etc.) gérés par des tiers et dont les droits d'accès sont gérés par un système de contrôle autonome et administrés par l'organisme tiers.
Dans certains cas le contrôle d'accès peut s'appuyer sur les informations de sécurité fournies par le SI de l'entreprise (identité et/ou rôle).

L'intégration avec ce type d'environnement peut être faite de deux manières :

- délégation complète d'administration des habilitations et d'authentification (Cf. Fédération d'identités § 4.1.15),
- provisioning du référentiel tiers.

Le développement constant des échanges commerciaux entre les partenaires via l'Internet est un facteur important de multiplication des infrastructures mettant en œuvre ce type d'interaction. Le besoin des possibilités d'intégration rapide des nouveaux partenaires a stimulé les multiples travaux de normalisation.

Le concept général d'architecture permettant l'interaction entre les systèmes autonomes des différents partenaires porte le nom de « Fédération des Identités ».

4.1.15 Fédération d'identités

Il est impossible d'aborder la fédération des identités d'une manière exhaustive dans ce document dédié à la gestion des identités d'un organisme et /ou d'une entreprise. C'est un sujet très vaste qui a fait l'objet de multiples travaux.

Nous nous limiterons par conséquent à une description générale en indiquant de quelle manière le système interne et autonome peut s'ouvrir à l'extérieur et collaborer avec des systèmes tiers.

La fédération consiste à faire communiquer plusieurs systèmes de gestion des identités, afin d'éviter de constituer une solution centralisée, tout en assurant des services d'authentification unique, d'échanges d'attributs et de droits utilisateurs entre les différents sites auxquels ils ont accès. À l'heure actuelle les solutions sont concentrées sur les technologies Web mais des travaux sont en cours pour étendre leur champ d'application.

Le diagramme suivant (Figure 3) présente la multiplicité des différentes initiatives et la convergence de tous ces travaux vers la normalisation autour de SAML 2.0.

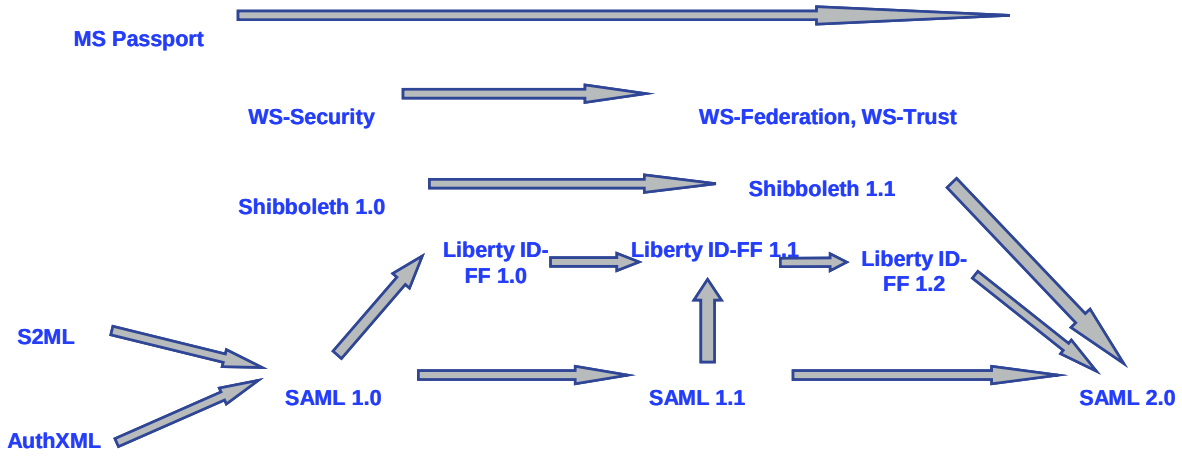

Figure 3 – Les « efforts » de normalisation

4.1.15.1 SAML

SAML (Security Assertion Markup Language) a été initialement conçu pour permettre, entre autres, la délégation d'authentification. C'est devenu un standard OASIS en 2002. Il s'agit d'un ensemble de spécifications qui définit comment des services peuvent échanger des assertions de sécurité (authentification, autorisation, attributs), indépendamment des technologies utilisées par chacun de ces services. SAML s'appuie sur des standards pré existants (XML, SSL, etc.) et a été conçu avec suffisamment d'abstraction pour rendre inter opérables des systèmes hétérogènes et s'articuler au mieux avec d'autres mécanismes de gestion d'identités.

4.1.15.2 Les concepts de fédération

Les approches de centralisation et de fédération sont parfaitement complémentaires :

- la gestion des identités centralisée est une première étape de rationalisation des informations au sein de l'entreprise/organisme,
- la fédération des identités répond aux besoins d'intégration des services d'identités entre différentes organisations (métiers, partenaires, fournisseurs, clients, etc.).

Les solutions de fédération d'identités s'appuient sur quelques concepts tels que :

L'identité fédérée :

- est un ensemble d'attributs fédérés, c'est-à-dire d'informations relatives à l'identité provenant de différentes sources et pouvant être mises en commun,
- apporte des gains fonctionnels :
  - pour l'utilisateur : la possibilité de partager son identité entre les différents systèmes,
  - pour l'entreprise : la possibilité de s'associer avec d'autres partenaires au sein d'une fédération, afin que les identités d'un domaine puissent donner accès aux services d'un autre domaine sans être obligé de mettre en œuvre une gestion lourde (et souvent pratiquement impossible) de gestion des identités des utilisateurs de chaque partenaire.

La répartition des responsabilités

La propagation d'identités et la fédération inter partenaires s'appuient sur une organisation tri partite (cf. Figure 4 ci-après) :

- un fournisseur d'identité (Identity Provider ou IDP) : chargé d'authentifier l'utilisateur et de gérer son identité (enregistrement, provisioning, gestion de comptes et de mots de passe),
- un fournisseur de services (Service Provider ou SP) : chargé de lui fournir des services en fonction de ses habilitations sur la base des informations fournies par le fournisseur d'identités à qui il fait confiance,
- l'utilisateur.

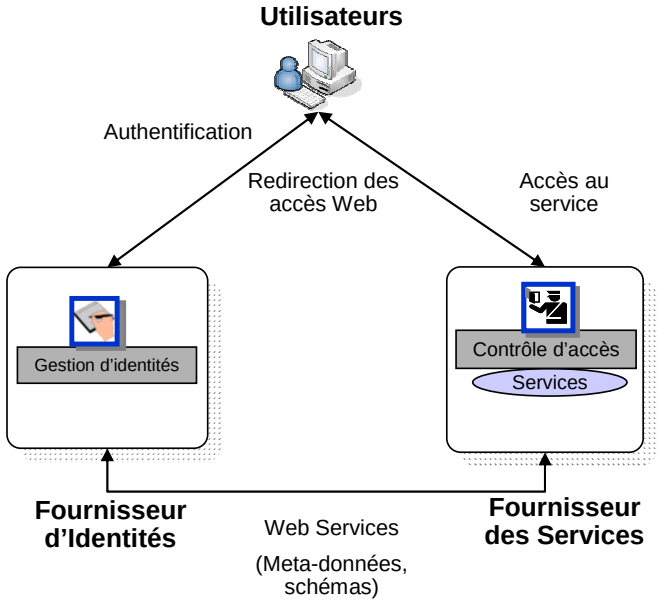

Figure 4 – Principe d'architecture de la fédération d'identités

Confiance entre les partenaires.

Tous les mécanismes de fédération d'identités se basent sur le principe fondamental d'existence d'une relation de confiance entre les partenaires qui ont décidé de collaborer.

Il est primordial que ces relations de confiance soient établies et gérés sur trois niveaux :

- **métier** où seront définis les services concernés par la fédération, les engagements de qualité de service et les conditions de mise en œuvre. En particulier le fournisseur de service pourra exiger une garantie de fiabilité et de niveau d'authentification de la part du fournisseur d'identité,
- **légal** où seront formalisées et contractualisées les exigences métier et définis les moyens et les procédures de résolution de cas de litiges,
- **technique** où seront définis les moyens techniques de mise en œuvre des liens sécurisés entre les sites, les formats de jetons de sécurité et les processus de validation de l'authenticité des informations échangées.

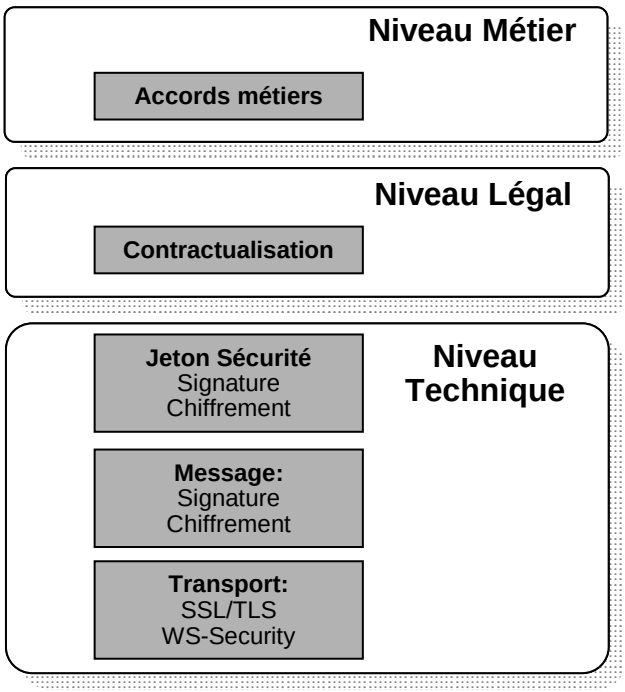

Figure 5 – Principes des relations de confiance

La gestion d'identités fédérées ou Federated Identity Management (FIM)

- est une façon standardisée de gérer de bout en bout le cycle de vie des identités, au sein de l'entreprise et entre les entreprises,
- elle permet :
  - d'étendre les pratiques de gestion des identités de l'entreprise,
  - de simplifier la gestion des identités au-delà des frontières de l'entreprise,
  - de faciliter l'intégration métier des partenaires via des relations de confiance et le partage d'information dans un environnement sécurisé.

La gestion FIM se base sur les définitions suivantes :

- le mapping d'identités/attributs définit les attributs d'identités à partager et leur correspondance chez les différents partenaires
- la gestion/provisioning des comptes définit les processus de gestion d'information d'identités :
  - les informations à partager,
  - les informations que l'utilisateur peut gérer,
  - les informations qui peuvent être provisionnées automatiquement (a priori ou en temps réel),
- la jonction des comptes (Account linking) soit :
  - définit les processus de création et de suppression d'un lien entre un compte d'identité unique et les comptes de service chez les fournisseurs de service,
  - établit les liens entre les différents comptes de la même personne sur les divers sites des partenaires,
- la confiance définit les processus et les moyens utilisés pour assurer une communication sécurisée sur plusieurs niveaux :
  - connexions/transport,

- messages,
- jeton.

La gestion FIM met en œuvre les services suivants :

- le Web SSO inter-domaines ou SSO Fédéré – Accès interactif et sécurisé aux applications des partenaires qui met en œuvre les techniques de :
  - Push SSO : l'utilisateur accède d'abord au site de son IDP et est redirigé ensuite vers le SP,
  - Pull SSO : l'utilisateur accède au site du SP et est redirigé vers l'IDP si non authentifié,
  - SLO – Single Log Out : déconnexion de l'ensemble de sites ou l'utilisateur est autorisé d'accès,
  - WAYF : Le WAYF (pour Where Are You From?, « d'où êtes-vous ? ») est un service optionnel dont le but est d'orienter l'utilisateur vers son IDP,
- sécurité de Web Services – Communication sécurisée entre les applications conforme aux spécifications de OASIS « Web services security specifications »,
- gestion du cycle de vie d'identité - federated provisioning
  - Account linking à l'initiative de l'IDP,
  - Account linking à l'initiative du SP,
  - Provisioning du SP en temps réel (durant la phase de SSO),
  - Provisioning du SP « a priori » (durant la phase de gestion d'identités par l'IDP).

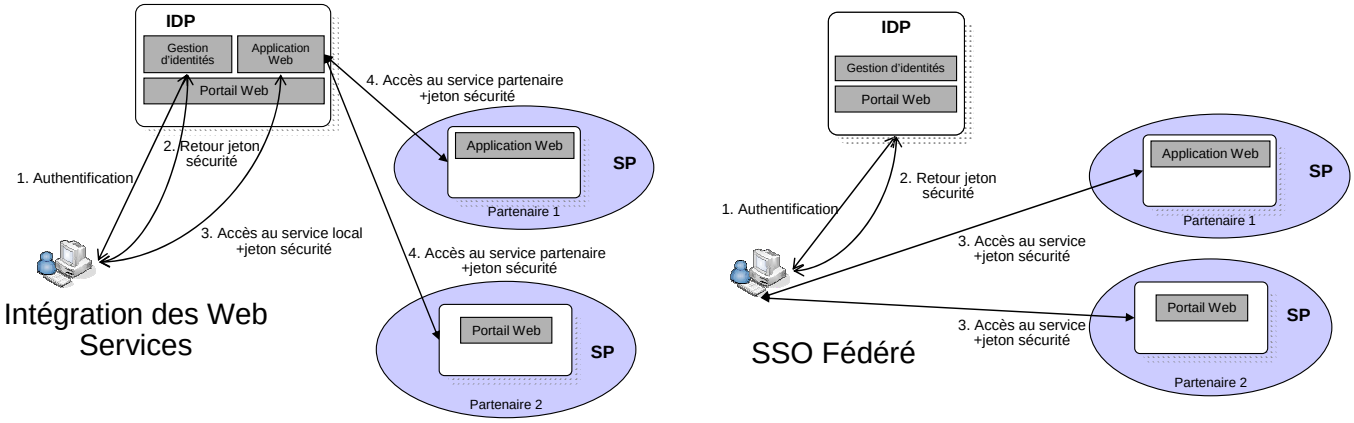

Figure 6 – Exemples de mise en œuvre de fédération des identités

Après cette présentation générale des concepts, les trois paragraphes introduisent les modèles théoriques de gestion des droits les plus répandus.

4.2. Modèle RBAC

Le modèle de sécurité RBAC (Role Based Access Control) est principalement issu d'Internet afin de prendre en compte des applications déployées sur de vastes organisations ou des applications inter-organisations (Extranet par exemple). Ce modèle permet en particulier de simplifier l'administration des droits et de prendre en compte la délégation de l'administration.

Les concepts du RBAC (http://csrc.nist.gov/rbac/) ont servi de base à la norme établie par American National Standard et référencée sous le N°:ANSI INCITS 359-2004 (approuvée le 19 Février 2004).

Ce modèle tend à se généraliser dans l'industrie et un nombre croissant de produits supportent un modèle d'habilitation "orienté rôles".

Le modèle RBAC se distingue du modèle DAC (Discretionary Access Control) popularisé par Unix. Le modèle DAC est centré sur les ressources physiques (fichier, exécutable, etc.) et identifie un propriétaire ainsi que des groupes d'utilisateurs ayant des droits sur la ressource (lecture, écriture, etc).

Le modèle RBAC modélise des fonctions métiers plutôt que des accès à des ressources informatiques. Un rôle correspond à une fonction au sein d'une organisation. Le principe de base du RBAC est que deux utilisateurs ayant les mêmes rôles ont les mêmes droits sur le système.

L'administration des rôles est ainsi facilement compréhensible par des administrateurs métiers et peut être déléguée. Les associations entre les rôles et les ressources physiques sont modélisées séparément par les concepteurs d'application et maîtrise d'ouvrage métier.

4.2.1 Modèle de base RBAC

Le standard propose un modèle de base (Core RBAC) ainsi que les extensions présentées dans les sous-chapitres suivants.

Les concepts manipulés par le modèle RBAC sont les suivants :

- USERS (Utilisateurs) : comptes permettant aux utilisateurs de se connecter au système,
- ROLES (Rôles) : fonctions métiers dans des organisations ou des périmètres donnés (par exemple : vendeur résidentiel dans l'agence X),
- OBS (Objets) : objets informatiques à protéger,
- OPS (Opérations) : opérations possibles sur les objets,
- PRMS (Permissions) : autorisation d'effectuer l'opération X sur l'objet Y,
- SESSIONS (Sessions) : session temporelle, chaque session est associée à un utilisateur pour une période de temps limitée,
- un utilisateur possède un rôle sur un périmètre donné,
- un rôle donne droit à des permissions,
- une permission est un ensemble d'opérations sur un objet,

- le contrôle d'accès se déroule au cours d'une session,
- au cours d'une session, il peut être nécessaire qu'un utilisateur n'ait qu'un et un seul rôle. C'est la notion de rôle actif,
- le périmètre est porté par un rôle et il est transmis de manière aveugle à l'application (la permission).

Note : le rôle est généralement accompagné par un périmètre (par exemple le numéro de compte client). La sémantique du périmètre est propre à l'application et n'est généralement pas contrôlée par le système de contrôle d'accès. Cette information est toutefois renseignée au cours du processus de déclaration des droits et participe pleinement aux contrôles de sécurité faits par l'application. Le système de contrôle d'accès joue simplement le rôle de courtier pour cette information.

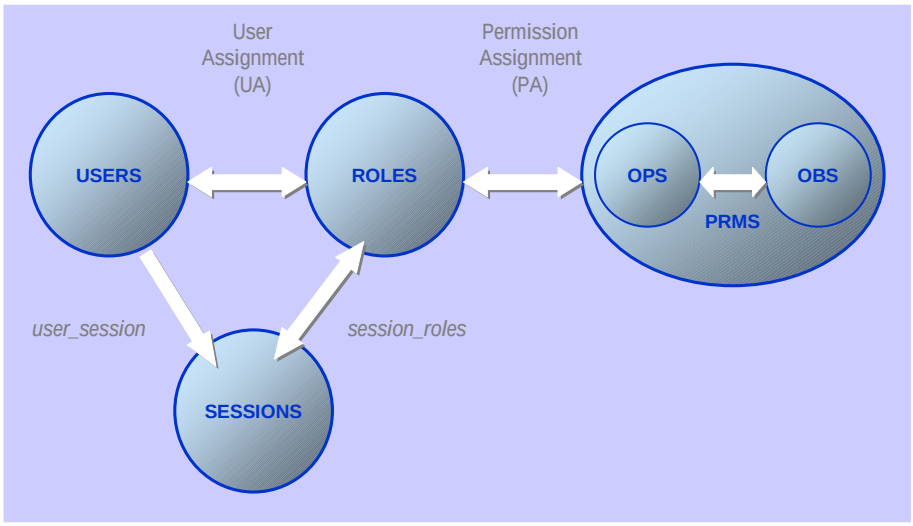

Figure 7 – Modèle de base RBAC

Principe de privilège minimum
Le fonctionnement de ce modèle et l'intégrité du système sont garantis si l'attribution des permissions respecte le principe de privilège minimum.

Ce principe exige que l'utilisateur ne dispose pas de plus de droits que nécessaire à son travail. Ce qui implique que les permissions affectées à un rôle constituent le strict minimum nécessaire à l'accomplissement des tâches relatives à ce rôle.

4.2.2 Modèle RBAC Hiérarchique

Le modèle RBAC hiérarchique (Hierarchical RBAC) ajoute au modèle de base le support de hiérarchie des rôles.

La hiérarchie établit les liens de parenté entre plusieurs niveaux des rôles et permet aux rôles « parents » de disposer des permissions attribuées aux rôles « enfants ».

Le standard admet deux types de hiérarchies :

- le **modèle hiérarchique général** (General Hierarchical RBAC) : cette variante établie des relations multiples entre plusieurs « parents » et « enfants »,
- le **modèle hiérarchique limité** (Limited Hierarchical RBAC) : cette version limite la relation à une simple structure d'arborescence. Ce qui veut dire qu'un rôle ne peut avoir qu'un seul « parent ».

Cette extension du modèle permet une administration plus efficace dans les grandes structures qui gèrent de très nombreuses permissions d'un grand nombre d'utilisateurs.
D'autre part ce principe permet de bien gérer les situations où certains rôles différents (du niveau supérieur) doivent bénéficier de certaines permissions communes.

***Remarque** : Très souvent on applique une version simple de l'extension au modèle hiérarchique limité. Elle admet une hiérarchie des rôles à deux niveaux. Le niveau 1 est appelé « un rôle » et le terme d'« un profil » sera utilisé pour le deuxième niveau. Le profil permettra donc les regroupements des rôles.*

4.2.2.1 Modèle RBAC avec contraintes

Le modèle RBAC avec contraintes (Constrained RBAC) ajoute au modèle la contrainte de séparation des pouvoirs.

Cette contrainte permet d'inclure dans le modèle la gestion de conflits d'intérêts et assurer que les utilisateurs bénéficieront des permissions selon la politique définie par l'organisation et ne pourront pas abuser de cumul non contrôlé de droits.

Séparation Statique des Pouvoirs (SSD - Static Separation of Duty Relations)

La contrainte de séparation des pouvoirs est utilisée pour assurer le respect de la politique des habilitations.

Un conflit d'intérêts peut arriver (dans un système du type RBAC) quand l'utilisateur obtient simultanément les droits associés à des rôles incompatibles.

Une méthode pour éviter cette situation est la mise en œuvre de séparation statique de pouvoir (SSD pour Static Separation of Duty).

L'exclusion mutuelle de certains rôles est spécifiée par les règles de SSD. Ces règles sont interprétées lors du processus d'affectation des rôles par l'administrateur et l'empêchent d'affecter des rôles incompatibles au même utilisateur.
De cette manière, à une personne qui bénéficie d'un rôle, on ne pourra pas affecter un deuxième rôle interdit par la règle de SSD.

Pour éviter les incohérences les règles SSD doivent prendre en compte les regroupements des rôles en fonction de leur hiérarchie.

Séparation Dynamique des Pouvoirs (DSD - Dynamic Separation of Duty Relations)

La séparation dynamique limite comme la SSD les rôles accessibles à un utilisateur.

Par contre le contexte est différent. La limitation n'est pas exploitée au moment de l'affectation des rôles mais au moment de leur activation dans une session.

Dans une même session, un utilisateur a la possibilité de ne pas activer tous ses rôles, mais uniquement le sous-ensemble de ses rôles nécessaires à la réalisation de la tâche à accomplir.

Ce mécanisme permet de garantir l'application des permissions minimales nécessaires dans une période d'exécution d'une tâche. On peut parler, dans ce contexte, de révocation temporaire des privilèges.

La mise en œuvre de ce mécanisme peut se révéler très complexe et le plus souvent n'est pas réalisée.

4.3. Autres modèles

D'autres modèles de sécurité existent, plus orientés ressources. Ces modèles tels que DAC et MAC sont très utilisés dans certains contextes (militaire) mais sont moins adaptés que le modèle RBAC à l'approche actuelle de la gestion des identités.

4.3.1 Modèle DAC

Le DAC (Discretionary Access Controls) est un modèle conceptuel dont le principe est de limiter l'accès à des objets en regard de l'identité des utilisateurs (humain, machines, etc.) et/ou des groupes auxquels ils appartiennent. Les contrôles sur une ressource sont dits discrétionnaires dans le sens où un utilisateur avec une autorisation d'accès définie est capable de la transmettre (indirectement ou directement) à n'importe quel autre utilisateur.

Ce modèle est principalement utilisé au sein d'implémentations informatiques car les notions développées sont surtout adaptées à la gestion d'accès sur des ressources informatiques. Ainsi, les implémentations adhérant à ce concept, doivent mettre en œuvre des mécanismes permettant d'enregistrer un ensemble de droits d'accès ou d'actions représentées sous la forme d'une matrice de contrôle d'accès.

Tableau 1 – Matrice de contrôle d'accès

	FichierLucas	**FichierLéa**
Lucas	rwx	r
Manon		r
Léa	r	rw

Parmi les différentes implémentations réalisées, les plus connues sont :

- **Protection Bits** : Popularisée par les systèmes Unix, cette implémentation représente la matrice de droits d'accès par colonne. Son principe consiste à définir pour une ressource si elle est partagée pour tous les utilisateurs, un groupe ou seulement son propriétaire,
- **Access Control Lists (ACLs)** : Le principe des ACLs implémente la matrice de contrôle d'accès par colonne en créant des listes d'utilisateurs pouvant accéder à la ressource et/ou des listes d'utilisateurs interdits d'accès à celle-ci,
- **Capabilities** : Comme pour les ACL une liste est créée, mais elle est liée à un utilisateur et non à une ressource, ainsi la représentation de la matrice est faite par ligne.

Ce modèle convient à des systèmes gérant l'accès d'objets peu sensibles et donne l'avantage de minimiser les coûts d'administration car celle-ci peut-être déléguée aux utilisateurs. Par contre, ses principes ne sont pas suffisants au sein d'une organisation qui a défini une politique de sécurité basée sur la sensibilité des ressources ou le profil métier des utilisateurs.

4.3.2 Modèle MAC

4.3.2.1 Introduction

En opposition avec le DAC où le propriétaire d'une ressource jouit de tous les droits sur une ressource qu'il a créée, le modèle Mandatory Access Control est utilisé quand la politique de sécurité d'une organisation définit que :

- les décisions de protection d'une ressource ne doivent pas être sous la responsabilité de son propriétaire,
- le système doit mettre en œuvre les mécanismes permettant de respecter la politique de sécurité et interdire au propriétaire d'une ressource d'agir à sa guise.

Afin d'aboutir à ces principes, ce modèle introduit la notion d'accès aux ressources en regard de la sensibilité des informations qu'elles contiennent et repose sur la labellisation systématique de ces ressources et des utilisateurs du système considéré. En hiérarchisant ces entités en plusieurs niveaux de confiance et sensibilité, puis en les labélisant en conséquence, on aboutit à une décomposition à laquelle il faudra ensuite ajouter des règles d'accès. On notera qu'un système informatique adhérant à ce principe est dit multi-level security (MLS).

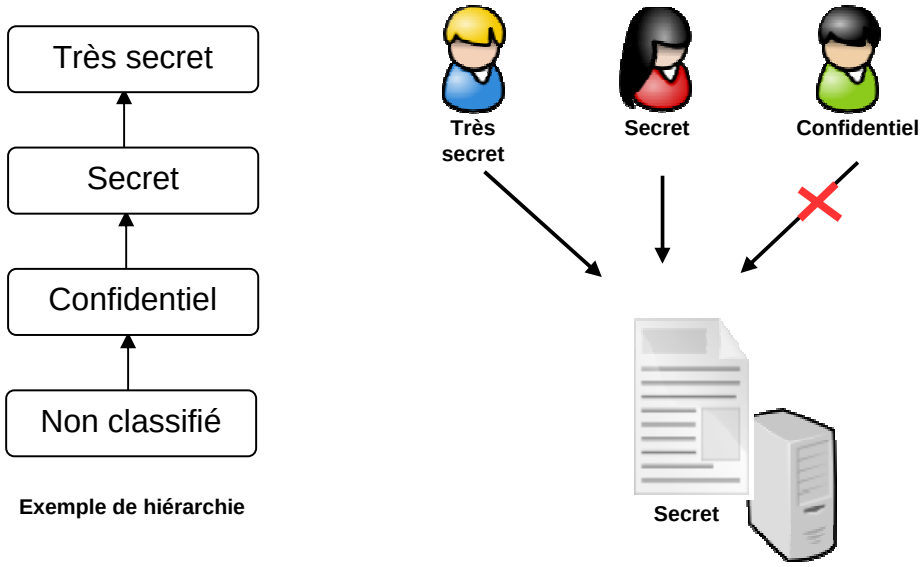

Figure 8 – Exemple d'habilitation

Les labels suivent une logique hiérarchique (ex : Confidentiel, Secret, Très secret, non classifié) et décrivent ainsi différents niveaux d'habilitation. Les droits d'accès aux ressources sont attribués en fonction du niveau d'habilitation de l'utilisateur et sont définis selon la problématique de sécurité à adresser : Confidentialité ou Intégrité.

4.3.2.2 Historique

L'émergence de travaux sur ce sujet date de la période de la Guerre Froide où la NSA a lancé différents projets visant à publier des référentiels pouvant être mis en application au sein des organisations gouvernementales américaines.

Confidentialité

La confidentialité est une des notions les plus importantes à orienter pour une organisation qui possède des données sensibles et faisant l'objet d'une classification. Le modèle de référence dans ce domaine est celui dit « Bell-LaPadula » développé par David Bell and Len LaPadula en 1973 pour formaliser la politique de sécurité multi-niveaux du « Department of Defense ». Celui-ci repose sur les règles suivantes :

- un utilisateur avec un niveau de confidentialité donné ne peut pas lire un objet avec un niveau de confidentialité plus élevé (no read-up),
- un utilisateur avec un niveau de confidentialité donné ne peut pas écrire sur un objet qui a un niveau de confidentialité moins élevé (no write-down).

En conséquence, avec Bell-LaPadula, les utilisateurs peuvent seulement créer un contenu à leur niveau de sécurité ou au-dessus (un utilisateur avec le niveau secret peut créer des documents secrets et top-secrets, mais pas des fichiers non classés).

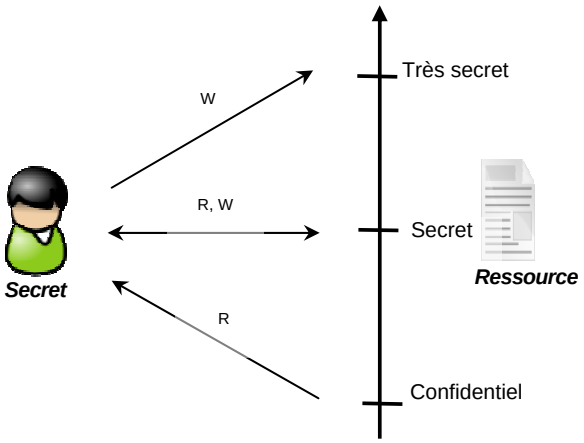

Figure 9 – Exemple du Modèle Bell-LaPadula

La confidentialité est atteinte par ce modèle en minimisant le nombre d'utilisateurs qui ont accès en lecture à des ressources classifiées à un niveau plus élevé que le leur.

Intégrité

Les modèles dédiés à l'intégrité des données ont fait l'objet d'un grand nombre de travaux à la fin du XX^{ème} siècle dont les plus connus sont Biba, Goguen-Meseguer, Sutherland, Clark-Wilson, Brewer-Nash (Chinese wall). Afin de simplifier ce chapitre, seul le principe de Biba dont les autres sont des extensions est présenté.

En opposition avec Bell-LaPadula, modèle de confidentialité, Biba définit deux grands principes qui se focalisent sur l'intégrité des données :

- un utilisateur avec un niveau de sécurité défini peut créer uniquement un contenu à son niveau ou en dessous (no write up),
- un utilisateur peut uniquement voir un contenu à ou au dessus de son niveau (no read down).

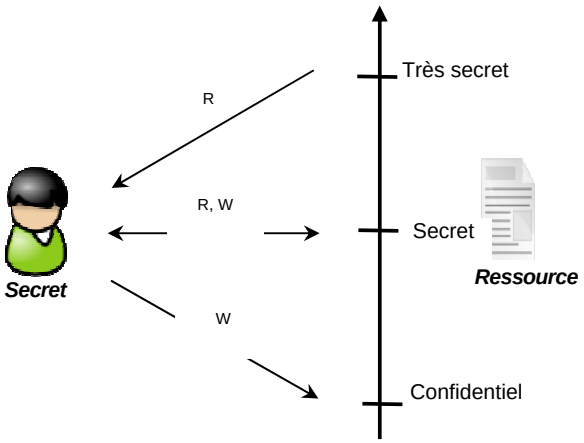

Figure 10 – Exemple du Modèle Biba

Grâce à ces principes, au sein d'une organisation pyramidale, le nombre d'utilisateurs pouvant modifier un document se voit limité et l'objectif d'intégrité est atteint.

4.3.2.3 Implémentation et relation avec RBAC

Au delà de ces principes et modèles associés, plusieurs éditeurs commercialisent des implémentations dédiées principalement aux organisations gouvernementales. D'autres projets comme SELinux et TrustedBSD visent à mettre respectivement les systèmes d'exploitation Linux et FreeBSD en conformité avec les Critères Commun qui entre autres supportent les modèles présentés.

Dans le cadre de l'entreprise, le déploiement de telles technologies s'avère particulièrement coûteux en études et surtout en exploitation et argumente le choix du modèle RBAC qui permet de mieux s'adapter au métier et au processus. Par contre, un compromis peut être trouvé en limitant le nombre de ressources (stratégie, finances) soumises à ces contraintes et en définissant des tables de corrélation entre le système multi-niveaux et celui supportant RBAC.

4.4. Modèle fonctionnel et de données

La suite de ce document reprend la terminologie introduite dans le paragraphe 4.1(les concepts). Dans un projet de gestion des identités, elle pourra être adaptée en fonction du modèle retenu.

4.4.1 Principes de fonctionnement

La gestion des habilitations est basée sur les principes suivants :

- tout accès au Système d'Information est conditionné par une authentification et une autorisation. *L'authentification peut être déléguée à un système tiers de confiance,*
- tout acteur du système est déclaré d'une manière unique dans un référentiel central de sécurité en tant que personne physique et peut disposer de comptes dans différents environnements et de permissions dans les applications en fonction des habilitations accordées. *La cohérence de ces informations est maintenue automatiquement par le système de gestion des habilitations,*
- **toute habilitation est attribuée en fonction du poste opérationnel au sein de l'organisation et non à titre individuel. Le poste opérationnel détermine les rôles et les périmètres nécessaires.** *Le poste opérationnel (position de travail) correspond à une fonction métier exercée au sein d'un élément de structure,*
- un utilisateur peut avoir un ou plusieurs profils. L'attribution se fait en fonction du poste opérationnel de l'utilisateur,
- un profil regroupe un ensemble de rôles nécessaires à l'exécution d'une fonction métier,
- un rôle définit les permissions nécessaires à l'utilisation d'une application ou des ressources,

- les définitions des rôles, profils ainsi que l'attribution des profils aux personnes se font via un outil central qui propage ensuite les informations nécessaires vers toutes les applications et environnements concernés. L'association personne / rôle applicatif (ou profil applicatif) est gérée hors application, lorsque l'application l'autorise. *Cela permet d'éviter d'avoir à développer une gestion des droits des utilisateurs dans l'application,*
- l'association personne / rôle applicatif est gérée de façon statique et explicite dans l'annuaire de sécurité (plutôt que de façon dynamique à base de règles de gestion organisationnelles). L'évaluation des droits, par le système de contrôle d'accès, doit être basée pour l'essentiel sur la consultation de ce rôle applicatif explicite (pas d'interprétation de règles complexes dans le processus d'autorisation),
- un contrôle permanent de l'adéquation des profils attribués aux rôles effectifs des personnes,
- la définition des droits d'accès aux ressources ou aux groupes de ressources est administrée dans les environnements cibles via les outils natifs de ces environnements. *Les administrateurs locaux continuent de gérer les ressources elles-mêmes et leurs associations avec les habilitations,*
- le contrôle d'accès lui-même est assuré soit par les composants du socle technique (cas de ressources et applications Web) soit par les mécanismes natifs des environnements (OS, NOS, messagerie, groupware, etc) soit par les applications.

Il est à noter donc que les informations nécessaires à la gestion des habilitations sont distribuées dans différents référentiels. On distingue :

- le **référentiel des habilitations**, référentiel mis à jour lors de la gestion des utilisateurs, des habilitations et des mots de passe,
- les **annuaires de sécurité**, qui ne contiennent qu'une partie des données du référentiel des habilitations (par exemple, les profils n'y figurent pas) et sont utilisés par les services d'authentification et d'autorisation, tels que :
    - Systèmes d'exploitation,
    - Sous systèmes de gestion des droits,
    - LDAP,
    - NOS (Network Operating Systems) et systèmes de partage des fichiers,
    - Messageries et systèmes collaboratifs.

4.4.2 Modèle de données

Le système de gestion centralisée d'habilitations doit permettre de modéliser les droits utilisateurs sur les ressources, (y compris les applications et les environnements). Cette modélisation passe par l'utilisation de rôles applicatifs, profils utilisateurs.

Cette modélisation doit permettre de fournir une visibilité « métier » des utilisateurs (le travail quotidien des utilisateurs). Cette visibilité sera fournie au travers des profils utilisateurs.

La Figure 11, ci-après explicite la modélisation des droits utilisateurs sur les ressources.

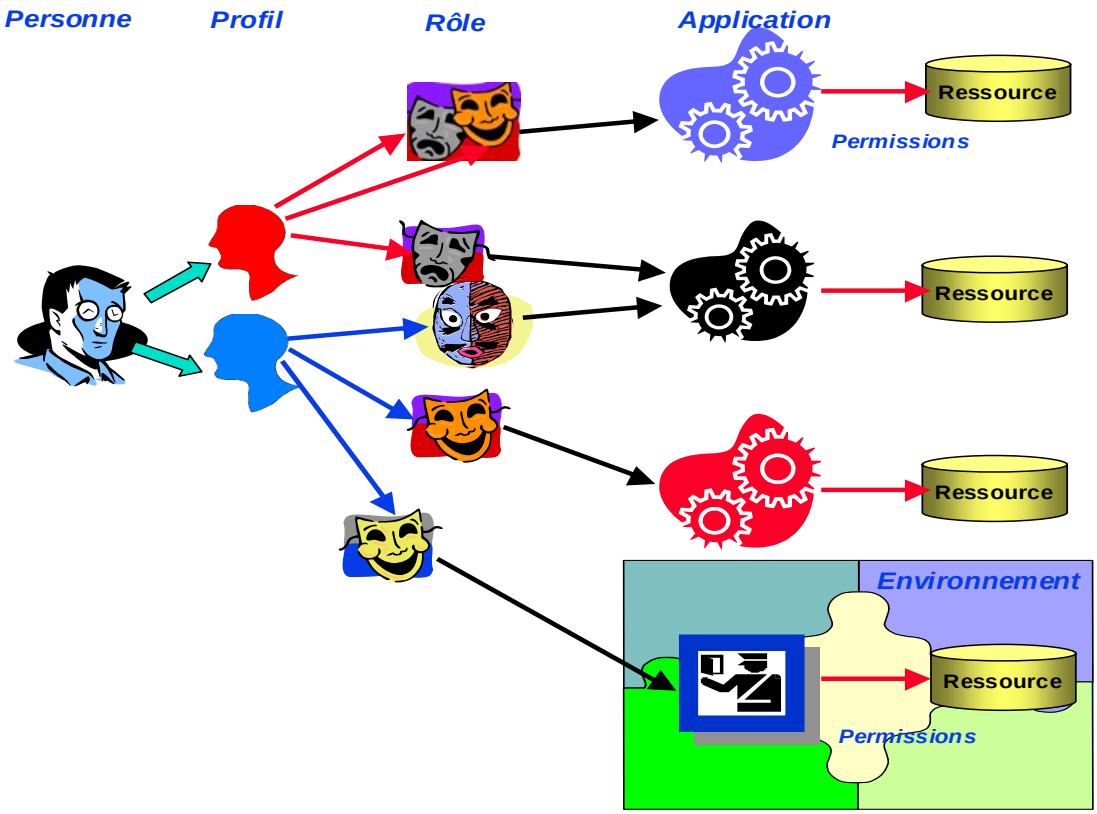

Figure 11 – Modélisation des droits utilisateurs sur les Ressources

Un service ou une application est décomposé en fonctions élémentaires appelées « ressources ». Un rôle applicatif est un ensemble de droits sur un ensemble de ressources :

- si l'autorisation a été entièrement déléguée (externalisée) par l'application, le rôle applicatif constitue simplement un droit d'accès aux ressources (typiquement droit d'accès à des URLs Web),
- si le système central se contente de fournir le rôle applicatif au service, c'est au service d'interpréter le sens du rôle applicatif. Des exemples typiques de rôle applicatifs sont : administrateur, administrateur délégué, utilisateur standard, etc. Un rôle applicatif ne peut cibler les ressources que d'un seul service.

Un profil utilisateur est un ensemble de rôles applicatifs. Un profil utilisateur se doit de décrire l'activité de l'utilisateur. Ce profil utilisateur permettra de lister l'ensemble des services que doit utiliser un utilisateur pour effectuer son travail quotidien. Afin d'éviter des re-saisies inutiles, on pourra ajouter des profils utilisateurs dits de « factorisation » :

- Profil « général » : décrit l'accès standard messagerie, pages jaunes, pages blanches, etc.,
- Profil « métier » : décrit l'ensemble des services accédés en standard par une personne appartenant à un métier.

Des contraintes de non cumul de pouvoir peuvent être associées aux rôles ou aux profils.

Ainsi, une personne pourra être associée à plusieurs profils utilisateur : profil général, profil métier(s).

4.5. Les processus et les acteurs

4.5.1 Les acteurs

Les principaux acteurs sont :

- l'utilisateur,
- l'administrateur du workflow,
- l'administrateur système et/ou services,
- l'administrateur de mots de passe,
- l'approbateur métier,
- l'approbateur technique,
- le propriétaire fonctionnel,
- les gestionnaires des ressources humaines internes et externes (DRH, gestionnaires de contrats, etc.),
- l'auditeur,
- le RSSI.

L'administrateur a pour responsabilité de gérer les profils correspondant aux fonctions rencontrées dans l'entreprise.

4.5.2 Les processus

Les principaux processus sont :

- la gestion des mots de passe,
- l'allocation des ressources (provisioning),
- l'administration et l'audit,
- la gestion des processus,
- la gestion des habilitations,
- le contrôle d'accès,
- la gestion personnelle (mots de passe, demandes d'accès, etc.),
- la réconciliation (association des comptes et des personnes, recherche de comptes orphelins, alertes et/ou correction des écarts).

4.6. Les fonctions et les services

4.6.1 Gestion des identités et des habilitations

La gestion centralisée des personnes et de leurs comptes d'accès sur toutes les applications et les environnements interfacés avec le système central d'habilitation fournit aux administrateurs une vue unifiée de l'ensemble des utilisateurs et de leurs attributs de sécurité.

La gestion des habilitations doit permettre de gérer le contenu du référentiel de sécurité. Elle se décline sous plusieurs aspects :

- la **gestion de personnes** (création, modification, suppression des comptes utilisateurs du référentiel central), grâce à :
    - une alimentation automatique du référentiel central à partir de référentiels tiers (fichiers du personnel, référentiels acteurs, structures, etc.) incluant utilisateurs internes et si nécessaire externes et partenaires, etc.,
    - une alimentation manuelle par des administrateurs centraux ou délégués,
- la **déclaration des gestionnaires** : désignation des gestionnaires fonctionnels qui interviennent sur la gestion fonctionnelle des personnes,
- la **déclaration des domaines d'administration** : périmètres de travail fonctionnel définissant un ensemble de populations géré par un gestionnaire. Ce périmètre pourra être de type géographique, métier, organisationnel. Dans certains cas, les périmètres de travail des gestionnaires peuvent se recouper.
  L'administration du référentiel de sécurité, qui se fait via :
    - la définition de niveau hiérarchique d'administration. Un niveau est attribué à chaque administrateur pour chaque processus d'alimentation,
    - la mise en place d'une fonction permettant à chaque administrateur de déléguer simplement tout ou partie de ses droits à un ou plusieurs autres administrateurs,
    - la déclaration des ressources applicatives ou services qui permet à un nouveau service ou application d'être déclaré dans le référentiel de façon à bénéficier du contrôle d'accès sur les ressources de l'application/service,
    - la déclaration des rôles, profils, groupes et périmètres. Cette déclaration permet de créer des profils et des rôles afin de permettre ensuite l'automatisation de la création et de la modification des comptes utilisateurs sur les systèmes et applications cibles,

  L'administrateur a pour responsabilité de créer les profils correspondant aux fonctions rencontrées dans l'entreprise. A chaque profil correspond un ensemble de rôles définissant la manière dont les comptes doivent être créés sur les plates-formes cibles.

  Toutes les déclarations peuvent être effectuées de manière interactive, mais également avec des moyens permettant de rejouer cette déclaration d'une plate-forme de test/intégration/pré-production vers une plate-forme de production sans risque d'erreur (par exemple, possibilité d'export de la déclaration),
- la **mise en œuvre des règles de gestion de mots de passe** définies pour chaque système et application cible (longueur, durée de validité, etc.) et respectant la politique de sécurité,

- création d'un système de « workflow » pour la gestion d'attribution, selon les règles préétablies, des profils et des rôles aux personnes (utilisateurs). Les principales fonctions du Workflow sont :
    - l'affectation d'un profil à un utilisateur,
    - la suspension ou suppression d'un utilisateur,
    - l'activation d'un utilisateur,
    - le changement de profil (changement des habilitations),
    - la réinitialisation / changement d'un mot de passe sur l'ensemble des comptes propres à l'utilisateur,
    - la délégation des droits opérationnels ou d'administration,
    - la modification de la configuration du système de workflow.

4.6.2 Alimentation avale (Provisioning)

Le système de gestion des habilitations est le point central d'alimentation des comptes (identifiant, mot de passe, autres attributs) pour des environnements techniques et des applications du Système d'Information. Dans certains cas (comme l'initialisation), des informations pourront être remontées des environnements.

Le provisioning permet d'alimenter les référentiels utilisateurs des services cibles à partir du référentiel central mais aussi de détecter des modifications des référentiels. Le provisioning permet de répondre aux besoins suivants :

- association d'une fiche personne à un ensemble de comptes,
- calcul automatique de certains attributs des comptes à partir d'autres comptes ou des attributs de la fiche de personne,
- pour les attributs ne pouvant être calculés automatiquement, et étant propriété du référentiel cible, leurs valeurs devront être remontées du référentiel cible pour consolidation dans le référentiel central,
- toute modification dans le référentiel central sur un compte doit être répercutée sur le référentiel cible associé au compte,
- toute modification effectuée en direct sur un référentiel cible doit être remontée sur le référentiel central ; si la modification est autorisée, celle-ci est consolidée au sein du référentiel central, et répercutée si nécessaire sur les autres référentiels cibles (changement de mot de passe, changement d'adresse e-mail) ; si la modification est non autorisée, la modification effectuée sur le référentiel cible doit être écrasée avec l'ancienne valeur stockée dans le référentiel central (comme toute autre action de provisioning, cette action devra être tracée),
- tout compte sur un référentiel cible non rattaché à une personne doit pouvoir être détecté,
- tout compte dont un attribut ne respecte pas la règle de création doit pouvoir être détecté ; toutefois, la règle de création doit pouvoir accepter les exceptions de sorte à pouvoir prendre en compte l'historique des comptes actuels.

4.6.3 Le service de changement et de synchronisation des mots de passe

Ce service permet de garantir la conformité à la politique de gestion des mots de passe en vigueur. La conformité est vérifiée en amont et propagée ensuite. De cette façon les mots de passe de tous les environnements respectent la même politique générale.

Il est possible également d'intercepter les demandes de changement des mots de passe initiées dans certains environnements. Dans ce cas le nouveau mot de passe est dirigé vers le service central qui le distribue selon le mode standard.

Par le même mécanisme, l'administrateur peut également forcer un nouveau mot de passe pour un utilisateur. Ce mot de passe doit être obligatoirement changé à la première connexion. Le système offre un service du changement global de mot de passe accessible depuis le réseau de l'entreprise et un service de réinitialisation via une interface spécifique (réinitialisation du mot de passe à l'aide de challenges (questions/réponses) statiques ou dynamiques) ou via un Help Desk.

Ce service permet à l'utilisateur de demander en une opération le changement de mot de passe dans tous les environnements auxquels il peut accéder en fonction de son métier dans l'entreprise.

4.6.4 Processus et mécanismes de contrôle d'accès et d'évaluation des droits

Tout accès au Système d'Information est conditionné par une authentification et une autorisation.

4.6.4.1 Authentification

Le système de gestion des identités offre un service d'authentification pour les applications et les environnements SI. Une requête contrôle, dans l'annuaire de sécurité, l'existence du compte de la personne, le mot de passe (ou les crédentiels d'autre nature) et le statut du compte.

Le service d'authentification peut être fourni par plusieurs composants différents en fonction d'environnement ou d'application. La cohérence des tous les annuaires de sécurité est assurée par le système central de gestion des identités.

De plus, en complément de celui-ci, le service d'authentification permet principalement :

- de réaliser une fonction de SSO (Single Sign On) pour améliorer le confort des utilisateurs,
- de coopérer avec un ou des systèmes d'authentification forte (PKI, Biométrie, Carte à puce, Clé USB, Token, etc.),
- de coopérer avec un ou des systèmes d'authentification tierce pour déléguer l'authentification à un système tiers de confiance,

- de pouvoir imposer en fonction de la ressource, du périmètre temporel et géographique, un mode d'authentification pour cette personne.

4.6.4.2 Autorisation

Après la phase d'authentification des utilisateurs, le système pourra autoriser ces utilisateurs sur l'environnement technique ou l'application auquel ils tentent d'accéder par le contrôle de leurs droits d'accès.

Le service d'autorisation est chargé d'évaluer les droits effectifs sur la base des informations (identité et preuves d'authenticité) fournies par le service d'authentification.

Le contrôle d'accès lui-même est assuré soit par les composants du socle technique (cas de ressources et applications Web) soit par les mécanismes natifs des environnements (OS, NOS, messagerie, groupware, etc.) soit par les applications.

Les modes d'autorisation supportés peuvent être classés de la manière suivante:

- **autorisation en entrée du réseau** : le système de gestion des identités permet ou non l'accès (l'ouverture de session) à l'infrastructure d'accès à l'ensemble de services supportés en amont de l'application. L'évaluation se fait en fonction de l'utilisateur, du périmètre temporel, périmètre géographique et de la typologie de sa tentative d'accès. Le service d'autorisation d'entrée réseau est chargé également de gérer les connexions des utilisateurs une fois le contrôle d'autorisation réalisé. Des paramètres de connexion (timer de déconnexion après inactivité, durée maximum de connexion…) spécifiques seront contrôlés en fonction de l'utilisateur, de la ressource à laquelle il accède, du périmètre temporel, géographique et/ou de sa typologie d'accès,
- **autorisation de type Rôle / Ressource/ Application** : autorisation de type simple : accès ou non au service (en fonction du rôle de l'utilisateur, du périmètre temporel, périmètre géographique et du mode d'authentification de sa tentative d'accès). Les ressources du service cible sont modélisées dans le référentiel et c'est le système de gestion des identités qui permet ou non l'accès à ces ressources (filtrage des URLS des pages Web statiques ou dynamiques). Dans le cas d'applications capables d'appliquer le modèle RBAC (comme les rôles J2EE) le système de gestion des identités positionne les rôles et les droits effectifs sont évalués par l'application elle-même,
- **autorisation Environnement** : D'une manière générale, les autorisations des environnements non Web sont validées par les mécanismes natifs déjà présents. Ainsi ce sont les OS, NOS, messagerie, groupware qui contrôlent les droits d'accès à leurs propres ressources (système de fichiers, imprimantes, transactions, etc.) sur la base des informations détenues dans leurs structures de sécurité internes. Ces informations sont mises à jours, d'une manière cohérente avec les rôles des utilisateurs, par le service de gestion centrale des habilitations. La définition des droits d'accès aux ressources ou aux groupes de ressources en fonction des rôles (modélisées en tant que groupes) est administrée dans les environnements cibles via les outils natifs de ces environnements,
- **autorisations externes :** Les systèmes externes partenaires peuvent autoriser l'accès à leurs ressources tout en déléguant au SI d'entreprise l'authentification de la personne

et le processus de détermination du rôle actif de la session en cours. Le système de l'entreprise prend en charge l'authentification de la personne et la recherche du rôle actif de l'application demandée. Ce rôle et l'identité sont communiqués au système externe par un jeton via un canal sécurisé. Les modalités et les mécanismes précis peuvent varier en fonction du système du partenaire. Ces mécanismes feront souvent appel aux solutions de fédération d'identités telles que décrites précédemment.

5 - Démarche

La mise en œuvre d'un système de gestion des identités s'inscrit globalement dans un cadre classique d'un projet informatique. Toutefois, par son caractère transverse à la fois sur le plan fonctionnel et technique, ce type de projet impose une démarche adaptée dont les grandes lignes sont présentées dans ce chapitre.

Les facteurs clés critiques du succès d'un projet de gestion des identités sont d'abord d'ordres fonctionnels et organisationnels :

- identification des référentiels sources de données personnelles pour les différentes populations (internes, externes, clients, etc.). A noter que ces référentiels doivent être fiables,
- définition des profils métiers et des rôles liés aux outils nécessaires à l'exécution des tâches associées et indépendants d'organisation hiérarchique,
- désignation ou mise en place d'un organisme (comité inter-métiers, organisation du travail, direction des risques, etc.) responsable de la validation de définition des rôles, des profils et des règles de leur affectation,
- définition des règles de séparation des pouvoirs (conformité aux réglementations du secteur d'activité),
- identification et formalisation des processus de gestion du cycle de vie des droits (arrivée, départ, mutation d'une personne), des règles d'approbation, etc.,
- engagement fort de la Direction Générale indispensable pour le pilotage d'un projet transverse.

Il est à noter que certaines normes ou codes de bonnes pratiques (tels que l'ISO 17799, l'ISO 2700x, etc.) abordent, voire justifient la gestion des identités et des droits d'accès.

5.1. Définition du périmètre

Le périmètre d'un projet de gestion des identités et de contrôle d'accès pour une organisation donnée doit prendre en compte :

- les activités métier et leurs propres règles de sécurité,
- les différentes populations concernées (personnel interne, prestataires, fournisseurs, visiteurs, intérimaires, auditeurs, etc.),
- les processus de définition et d'attribution des droits,
- les ressources prises en compte :
    - ressources à protéger (locaux, serveurs, composants techniques, applications, bases de données, documents, etc.),
    - ressources attribuées (PC, téléphone, PDA, carte à puce, etc.).

Un périmètre plus restreint peut être envisagé dans une première phase du projet pour en faciliter la mise en œuvre progressive (par exemple en considérant comme prioritaires des domaines métiers ou des populations).

5.2. Les acteurs du projet

Un projet de gestion des identités et de contrôle d'accès est transversal et concerne de nombreux acteurs internes, voire externes.

5.2.1 Principaux acteurs du projet

Le sponsor
C'est une personne qui dispose d'un haut niveau de décision (idéalement, il fait partie de la Direction Générale) et soutient le projet au travers :

- d'une communication adaptée à l'ensemble des parties prenantes du projet,
- de validation stratégique tout au long du projet.

Le Maître d'Ouvrage du projet
C'est le commanditaire du projet. Il peut s'agir des Ressources Humaines, d'une Direction Métier ou de la Direction des Systèmes d'Information.

Il est possible que ce soit la même personne que le sponsor.

L'équipe projet (Maître d'œuvre du projet)
Elle doit associer des compétences métier, en organisation, en architecture de Système d'Information et en sécurité.

Les propriétaires fonctionnels
Ils sont considérés comme les propriétaires des ressources et des processus à protéger. Ils définissent et valident les profils, les rôles et les droits associés ainsi que leurs modalités d'attribution. Cette définition exige une vision globale et une acceptation générale. Il est donc nécessaire qu'une entité réunissant tous les métiers de l'entreprise ou de l'organisme et disposant de l'autorité nécessaire pour entériner les choix soit chargée de piloter cette activité.

Il peut être nécessaire de la créer pour le besoin du projet si aucune entité existante ne dispose de cette capacité. Comme mentionné en introduction de ce chapitre, c'est un facteur clé de réussite d'un projet de gestion des identités.

Les gestionnaires du personnel interne et des intervenants ou utilisateurs externes
Étant responsables des référentiels de données personnelles, ils participent à la définition et à la validation des interfaces avec leurs systèmes.

La Direction des Systèmes d'Information
Elle a en charge la gestion des différents systèmes et contribue à la conception des solutions et à leur intégration.

Le RSSI
Le RSSI vérifie les solutions en s'assurant que le niveau de sécurité est conforme aux exigences de l'entreprise.

Une fois le projet terminé (voire en cours de projet), il audite et valide la bonne mise en œuvre du système de gestion des identités et des droits d'accès.

5.2.2 Autres contributeurs au projet

L'organisation
Lorsqu'il existe, le service de l'organisation valide les circuits d'attribution. Dans le cas contraire, cette validation est effectuée par les Directions Fonctionnelles.

Le service juridique
Il vérifie la conformité des solutions aux exigences légales et valide les clauses de partage des responsabilités des différents acteurs externes.

Les prestataires en cas d'externalisation de services
Leurs engagements doivent intégrer les nouvelles règles et dispositifs de gestion des droits. Dans certains cas il peut arriver que les contrats d'externalisation doivent être modifiés puisque les domaines de responsabilité changent. Le prestataire pourra, par exemple, être toujours en charge de l'infrastructure mais ne maîtrisera plus le processus de gestion des droits, qui ne sera plus sous sa responsabilité, mais qui sera opéré par le système central.

Les partenaires
En cas d'ouverture des Systèmes d'Information aux partenaires (clients, fournisseurs, etc.), ceux-ci sont associés à la définition des règles d'accès et des interfaces.

5.3. Les étapes standards

Le système de gestion des identités apporte le service de gestion centralisé et, en principe, ne doit pas modifier le fonctionnement des systèmes et/ou applications qui seront provisionnés. La phase d'étude de l'existant doit donc être la plus complète possible pour permettre une intégration avec un impact minimal sur le Système d'Information en place.

L'analyse critique de l'existant devra prendre en compte les domaines suivants :

- analyse de l'organisation :
  - recensement des utilisateurs et identification des référentiels sources d'approvisionnement des données personnelles,
  - identification des hiérarchies et de la réparation géographique,
  - identification des mouvements,
- analyse métier :
  - recensement des métiers et des populations concernées,
  - identification des applications et des règles de gestion des droits,
  - identification des profils existants et des processus de demandes, d'approbation et de déploiement,
- analyse technique :
  - analyse du mode de gestion des droits dans les applications / systèmes,
  - analyse de structure des données des annuaires et des bases de sécurité,
  - analyse de l'infrastructure : réseau, systèmes, technologies exploitées (annuaires, SGBD, etc.),

- prise en compte des contraintes
    - de sécurité,
    - de qualité de service,
    - de continuité.

Les données collectées permettront de démarrer les phases suivantes de conception et de spécifications.

La conception fonctionnelle

- définition du modèle des données et d'habilitation :
    - règles d'identification de personnes,
    - rôles (restrictions d'accès aux fonctions),
    - profils (regroupements et mise en cohérence des rôles),
    - périmètres (restrictions d'accès aux données),
    - etc.,
- définition des règles d'alimentation à partir des référentiels,
- définition des processus (workflow) de gestion du cycle de vie d'une identité et d'habilitation, tels que :
    - demandes et approbations des droits,
    - création, suppression, suspension/révocation des comptes,
    - gestion des approbateurs et des administrateurs,
- définition des processus de gestion des rôles et des profils (définition, validations, évolutions),
- définition des processus d'audit et de reporting,
- définition des règles de provisioning et de réconciliation des systèmes cibles,
- spécification des interfaces de connexion aux systèmes cibles,
- validation des aspects juridiques et réglementaires.

La définition de l'architecture technique et le choix des outils

L'élaboration de l'architecture technique, dont un modèle type est présenté dans le prochain chapitre, doit prendre en compte, en particulier, les aspects d'intégration aux différents systèmes cibles de contrôle d'accès.

La solution technique de gestion d'identités peut être construite sur la base d'un développement mais il faut savoir que dans ce domaine il existe, sur ce segment du marché, plusieurs produits performants qui permettent de satisfaire pratiquement tous les besoins fonctionnels.

Le choix d'un tel outil passe par les étapes classiques d'expression des besoins, de rédaction du cahier des charges et d'évaluation des produits. Il est également vivement recommandé de valider ce choix par le prototypage (création d'un POC, pour Proof Of Concept). Les principaux produits sont arrivés à une certaine maturité, mais la diversité des schémas d'annuaires cibles et des processus de gestion impose cette étape pour valider l'exploitabilité du produit dans un contexte particulier. D'une manière générale, les éditeurs et/ou intégrateurs se plient de bonne grâce à ce type de demande.

La réalisation et la mise en service

La réalisation est pilotée selon la méthodologie standard des projets informatiques.

Lors de la mise en service, quelques phases critiques doivent faire l'objet d'une attention particulière :

- l'alimentation initiale de la solution par les identités en provenance des référentiels d'utilisateurs. La qualité des données d'entrée est primordiale pour le bon démarrage. Elle devra être validée d'une manière précise avec les «propriétaires» des référentiels sources,
- la réconciliation initiale, phase critique par excellence. Elle permet d'aligner la vision centrale de la cible élaborée par la solution de gestion d'identités avec les données déjà présentes dans chacune des cibles originelles. D'une manière systématique ce processus permet de constater de nombreux écarts et de les résoudre en appliquant les règles établies préalablement. Les erreurs dans ce traitement peuvent potentiellement perturber fortement la production. Ces processus doivent donc être répétés et validés minutieusement, d'autant plus qu'ils devront s'exécuter sur une période la plus courte possible, de faible activité et de stabilité des informations incluses dans les annuaires,
- la conduite du changement. L'introduction d'une solution de gestion d'identités produit nécessairement des changements dans plusieurs modes opératoires et bouscule les habitudes des utilisateurs et/ou des administrateurs. C'est pourquoi, si l'on veut que le projet soit une complète réussite, elle devra être accompagnée d'une gestion de changement rigoureuse avec un support spécifique sur la période du déploiement.

Le maintien en condition opérationnelle (MCO)

Comme tout projet informatique, le système de gestion des identités et des droits d'accès doit, une fois son intégration terminée, être maintenu en condition opérationnelle. Pour ce faire, il est nécessaire de prendre en compte les évolutions des applications et des référentiels.

De plus, l'outil mis en œuvre peut nécessiter d'éventuelles mises à jour fournies par l'éditeur. En particulier, les correctifs de sécurité seront systématiquement pris en compte.

5.4. Prise en compte d'un périmètre étendu

L'extension du périmètre de gestion des identités peut se traduire par différents cas d'ouverture du système vers l'extérieur :

- gestion d'identités des partenaires (entreprises clientes ou fournisseurs). Cette intégration peut s'effectuer selon deux approches :
    - référencement et intégration directe des utilisateurs désignés par le partenaire dans le système interne. Cette solution n'induit pas de changements majeurs dans le fonctionnement global. Les comptes des partenaires sont vus comme les comptes internes. Certaines procédures d'inscription, d'approbation et le nommage des comptes peuvent demander des adaptations. En contrepartie le partenaire est obligé de gérer ces utilisateurs dans son propre système et dans le système tiers. En effet, les procédures d'authentification et d'accès des deux systèmes restent totalement indépendantes,

- intégration de la gestion d'identités du partenaire via la fédération d'identités. Les principes de ce genre de solution ont été présentés dans les chapitres précédents. Sa mise en place demande des travaux d'adaptation d'architecture mais apporte la simplification des procédures de gestion et d'accès ainsi qu'une garantie de cohérence des informations de sécurité,

- gestion d'identités des clients individuels. L'intégration de cette population est plus difficile. Souvent elle est prise en charge par des solutions spécifiques ou des systèmes dédiés. Leur complexité se situe sur des plans différents. La gestion des utilisateurs internes concerne les populations moins nombreuses mais ayant l'accès à des systèmes multiples et des profils complexes tandis que la gestion des droits des clients individuels peut s'appliquer à des populations importantes mais avec des profils beaucoup plus simples ou portés par des systèmes intégrés. Cette démarche intéressera donc en premier lieu les entreprises / organismes ayant à gérer en direct des clients qui bénéficient d'une riche palette de services offerts par des architectures complexes et hétérogènes ainsi que les fournisseurs mettant en œuvre des services réalisés en collaboration avec plusieurs partenaires. Dans ce dernier cas de figure, ce sont les architectures du type « fédération d'identités » qui présentent le plus d'intérêt.

6 - Architecture

6.1. Introduction

Les chapitres précédents ont présenté les concepts, modèles, et méthodologie associés à la gestion d'identités et ont fait ressortir un ensemble de responsabilités devant être orienté par l'architecture informatique d'un organisme ou d'une entreprise. Cette architecture doit être conçue en fonction de la taille, de l'historique de l'infrastructure existante, des types d'utilisateurs et des implémentations géographiques.

6.2. Architecture fonctionnelle type

6.2.1 Les blocs fonctionnels

L'ensemble des concepts présentés préalablement est pris en charge par de nombreuses solutions disponibles sur le marché dont l'architecture fonctionnelle en règle générale peut être représentée par le schéma suivant (cf. Figure 12).

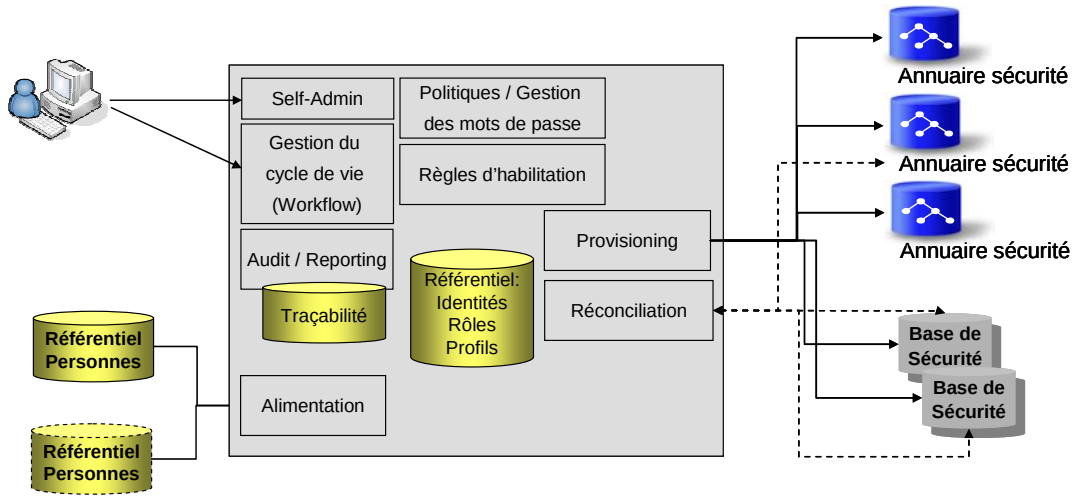

Figure 12 – Architecture fonctionnelle type

L'élément central est un référentiel interne qui héberge l'ensemble de données nécessaires à la gestion des habilitations. Parmi les informations principales on trouve les identités de tous les acteurs (utilisateurs, gestionnaires, administrateurs), les rôles, les profils, la structure organisationnelle, les règles et les processus de gestion, les règles de gestion de mots de passe. Un autre espace de stockage est dédié à la conservation des traces des actions de gestion des habilitations.

D'autres modules assurent la communication avec les éléments externes tels que les sources des données autoritaires en ce qui concerne les identités des personnes et les annuaires ou systèmes / bases de contrôle d'accès qui sont les cibles du provisioning.

6.2.2 Exigences de disponibilité

Les exigences de disponibilité d'un système de gestion d'identités ne sont en principe pas très élevées car, généralement, il n'intervient pas directement lors des contrôles d'accès. Ce système alimente d'une manière cohérente plusieurs systèmes de contrôle d'accès. En revanche, ces derniers doivent être très performants et hautement disponibles pour assurer la qualité du service du SI global.

L'interruption du fonctionnement du provisioning n'a pas d'impact fort sur le fonctionnement d'ensemble. Quelques fonctions peuvent éventuellement imposer des contraintes plus fortes. Notamment, les fonctions de self-service de changement du mot de passe et de déblocage des comptes dans le cas de son oubli. Mais là encore, le risque encouru est limité à l'impossibilité d'accès au SI d'un ou de quelques utilisateurs. Une analyse, de même qu'une évaluation des risques et des coûts des solutions devront déterminer au cas par cas si la haute disponibilité est réellement nécessaire.

6.2.3 Intégration dans le Système d'Information

L'architecture représentée préalablement prend en charge la gestion des identités et des habilitations de tous les utilisateurs identifiés d'un domaine précis. Ce domaine peut englober l'ensemble des ressources du Système d'Information d'une entreprise ou d'un organisme mais est souvent limité (dans les grandes structures) à un sous-ensemble de ces ressources.

On peut donc retrouver, dans certains cas, des architectures hiérarchiques où un système maître provisionne des systèmes esclaves chargés eux-mêmes de provisionner les ressources de leurs domaines. Le schéma suivant présente un exemple de ce type d'intégration.

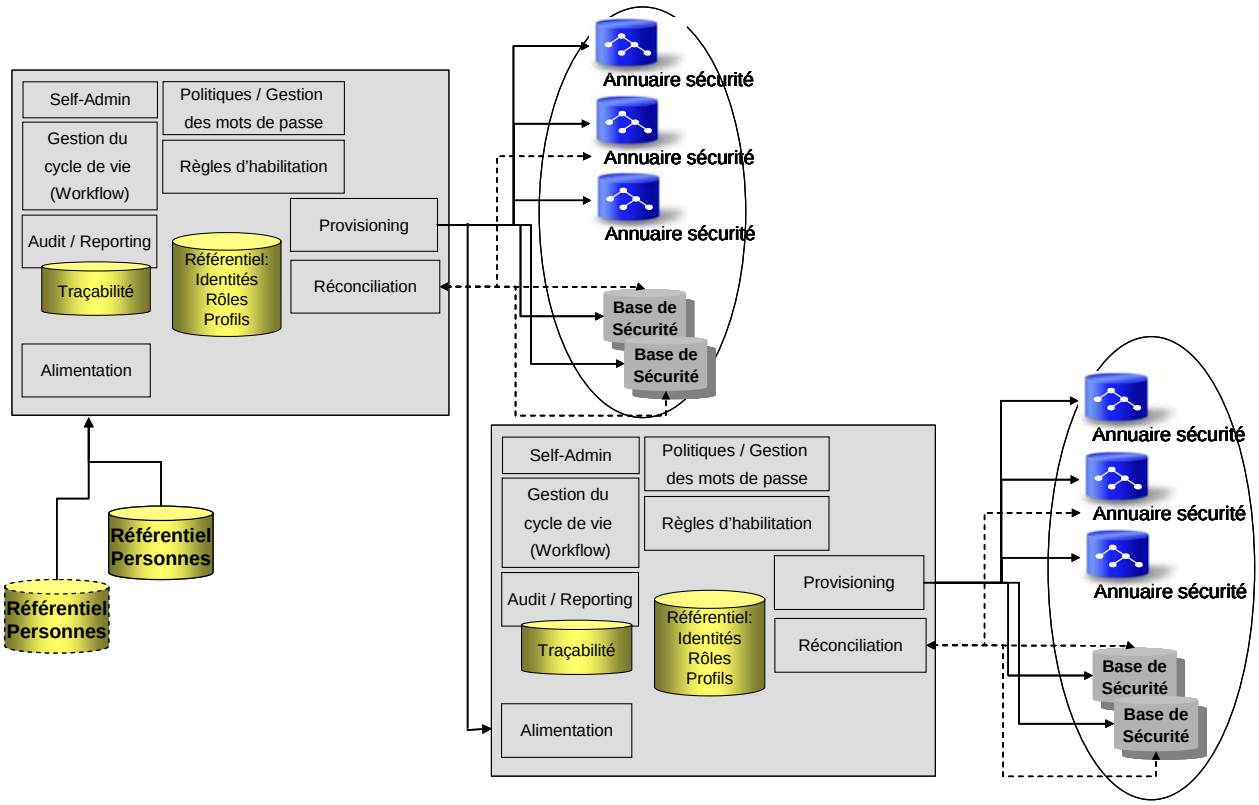

Figure 13 – Intégration dans le Système d'Information

L'infrastructure de gestion des identités s'inscrit dans un ensemble plus large qui apporte les fonctions supplémentaires nécessaires au contrôle d'accès aux SI qui sont essentiellement l'authentification, le SSO et les multiples systèmes du contrôle d'accès (évaluation des droits et autorisation) de l'entreprise ou de l'organisme.

L'ouverture sur Internet et la collaboration avec différents partenaires peut apporter en plus un besoin d'intégration avec les systèmes d'authentification tierce. La mise en œuvre de tels systèmes est basée de plus en plus sur les architectures de fédération d'identités.

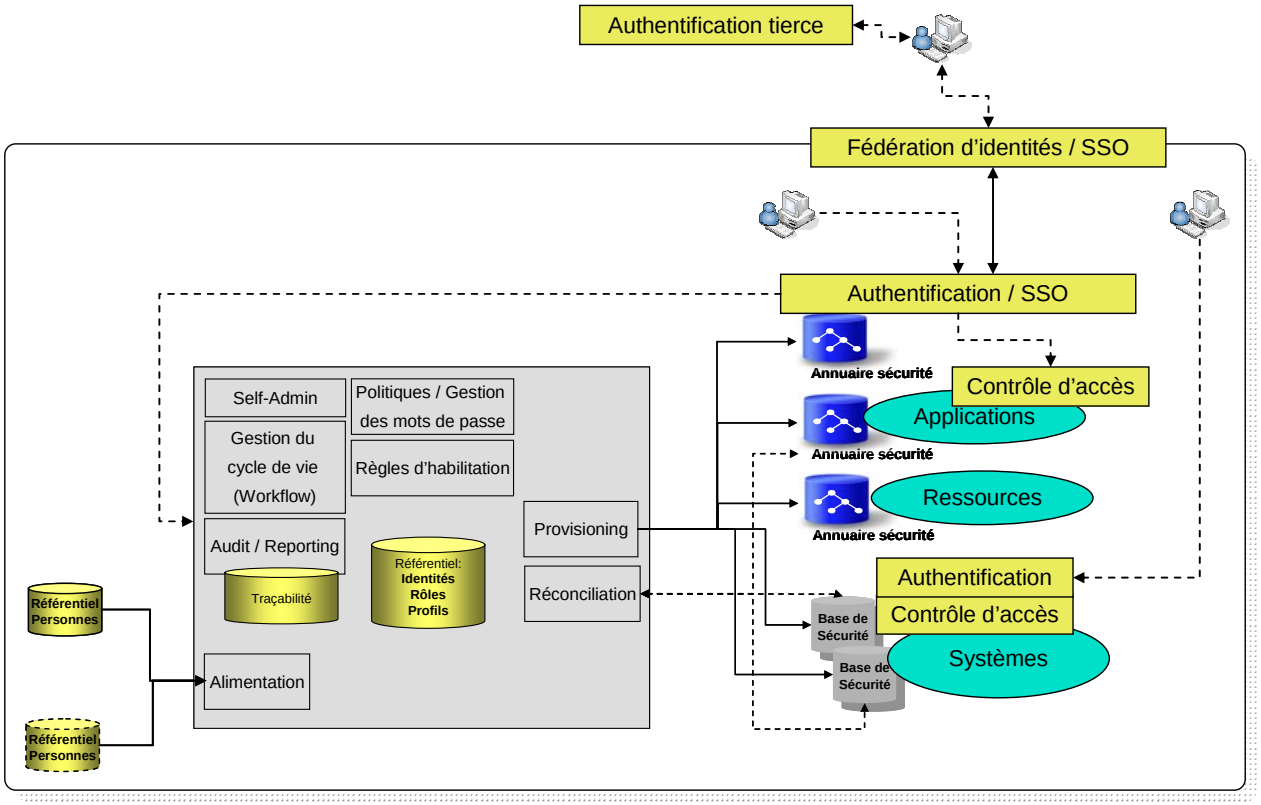

Figure 14 – Architectures de fédération d'identités

6.3. Architecture logique

Les solutions de gestion d'identités disponibles sur le marché sont réalisées sur la base des composants désormais classiques tels que les serveurs applicatifs Java, les bases de données relationnelles et les annuaires LDAP.

Il existe quelques exceptions chez les éditeurs « historiques » qui disposaient de solutions de gestion/synchronisation de comptes ou de provisioning réalisées en technologies différentes (code exécutable sur des plates-formes Windows ou Unix et client lourd). Ces solutions sont également en train d'évoluer vers les architectures Java et HTML.

Le schéma suivant (cf. Figure 15) présente un exemple d'architecture logique d'intégration d'un système de gestion d'identités. Il n'a pas vocation à être exhaustif mais illustre l'interaction entre les principaux composants et les protocoles d'échange avec les systèmes environnants. Les différentes solutions du marché peuvent mettre en œuvre des combinaisons variées des mécanismes de provisioning et d'alimentation.

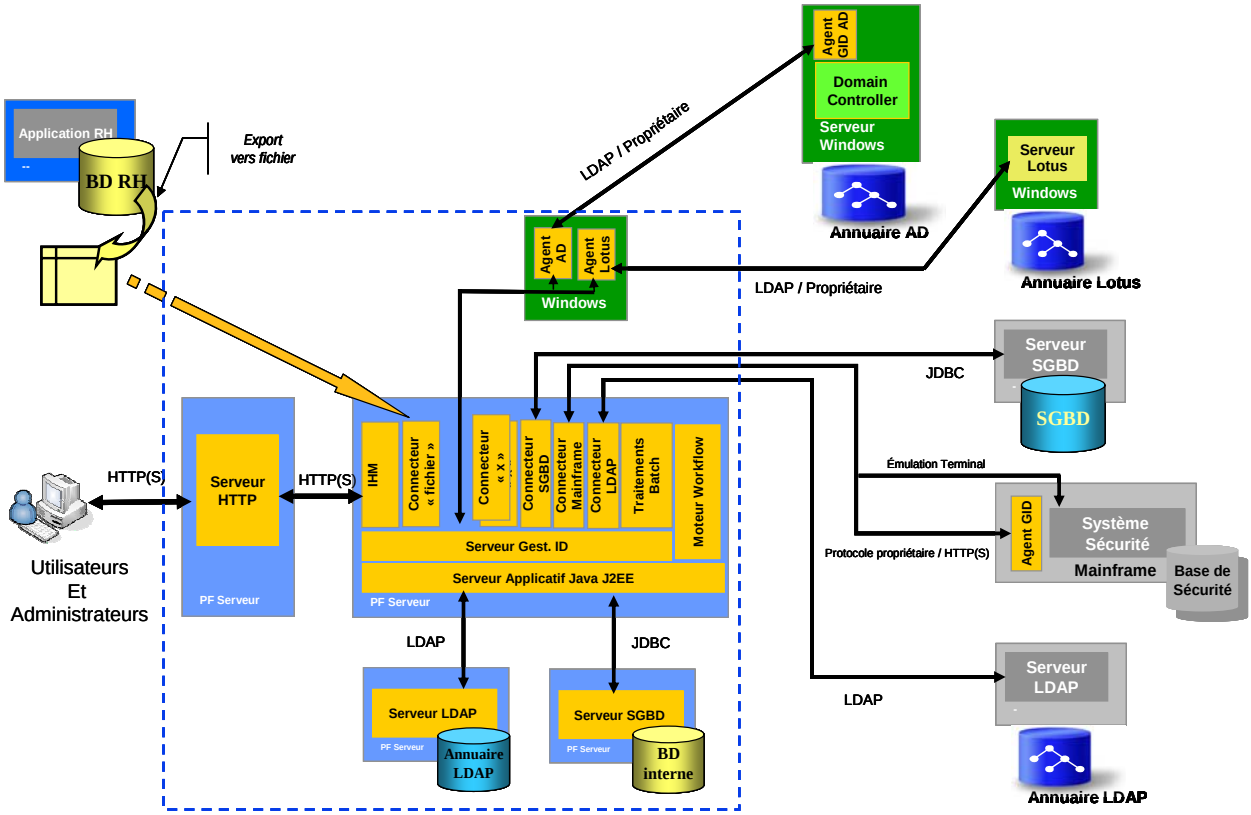

Figure 15 – Architecture logique d'intégration d'un système de gestion d'identités

6.4. Standards et Technologies de mise en oeuvre

6.4.1 Alimentation

Dans notre exemple d'architecture, l'alimentation du référentiel interne est effectuée par l'intégration du fichier extrait de la base de données RH. Ce mécanisme est souvent utilisé ; en effet, les autorités qui gèrent ces systèmes sont souvent réticentes quant à l'intégration directe et la détection de changements dans les bases RH.

D'autres possibilités d'alimentation de la base de gestion des identités sont offertes grâce à l'utilisation :

- de connecteurs LDAP – applicable par exemple dans le cas d'un référentiel « acteurs » sous forme d'annuaire LDAP d'entreprise,
- de connecteurs aux annuaires propriétaires,
- de connecteurs SGBD génériques (avec le paramétrage adapté),
- de connecteurs spécifiques pour les ERP de gestion de ressources humaines,
- de protocoles standardisés tels que SPML (Service Provisioning Markup Language) ou DSML (Directory Services Markup Language).

6.4.2 Hébergement des données

Le stockage des données nécessaires à la gestion d'identités s'appuie soit sur les bases de données relationnelles, soit sur les annuaires LDAP ou X500. Certains produits exigent la présence de deux supports en même temps. Cette contrainte peut se justifier parfois par la volonté d'adaptation du média par rapport à la nature de données hébergées (l'annuaire pour les données personnelles, organisationnelles et les habilitations, SGBD pour les données de traces et du reporting).

6.4.3 Accès utilisateurs

Comme l'indique la Figure 15 la tendance générale est de fournir l'accès via le client léger et HTTPS (protocole obligatoire puisque les données véhiculées sont des données de sécurité) pour toutes les interfaces fonctionnelles.

Pour des raisons historiques certains progiciels proposent encore des consoles du type client lourd. Leur utilisation est fortement déconseillée pour des raisons évidentes de contraintes de gestion de leur déploiement.

Elle peut être néanmoins acceptée dans le cas de certaines interfaces d'administration techniques utilisées par une population peu nombreuse.

6.4.4 Provisioning

Les moteurs du provisioning dialoguent avec les systèmes cibles via les connecteurs adaptés aux protocoles et caractéristiques des environnements gérés.

Les technologies utilisées peuvent être classées dans les catégories suivantes :

- connecteurs LDAP : capables de gérer toutes les cibles qui supportent le protocole LDAP nativement ou via les interfaces supplémentaires,
- connecteurs SGBD : connecteurs adaptés aux protocoles d'accès des SGBD, ayant la connaissance et capables de provisionner leur modèle de sécurité interne,
- connecteurs SGBD génériques : connecteurs offrant la connectivité via les pilotes standards tels que JDBC/ODBC et capables de provisionner, après paramétrage personnalisé, le contenu des tables de bases de données,
- connecteurs CLI : connecteurs « Commande LIgne » sont utilisés dans les cas de gestion d'environnements particuliers pour lesquels il n'existe pas de connecteurs adaptés. Après la connexion au système cible, ils déclenchent l'exécution des commandes système ou des scripts pour provisionner les structures spécifiques,
- connecteurs SPML : ce protocole, déjà cité dans le cas d'alimentation amont, peut être utilisé également pour gérer les cibles qui le supportent,
- connecteurs spécialisés : beaucoup d'environnements, ERP, systèmes sont accessibles uniquement via des protocoles natifs spécifiques. Des listes de connecteurs de ce type, plus ou moins riches, sont proposées par tous les progiciels.

Certains de ces connecteurs peuvent être hébergés directement sur les plates-formes serveurs et d'autres exigent parfois des passerelles spécifiques puisque l'accès aux systèmes cibles s'appuie sur les API disponibles uniquement sur un type d'OS donné.

Il faut signaler que certains connecteurs accèdent à distance à leur cible (un compte d'accès privilégié est nécessaire) tandis que les autres communiquent avec un agent résidant intégré à la cible. Cette technique apporte parfois des fonctionnalités plus riches mais elle est intrusive et nécessite la gestion du déploiement de ces agents.

Les deux modes d'accès ont leurs faiblesses et leurs points forts. Certains éditeurs proposent pour certaines cibles un connecteur de chaque type laissant le choix au client ou à l'intégrateur.

6.4.5 Contrôle d'accès

L'accès aux outils de gestion d'identités est un aspect important à considérer. Les progiciels proposent par défaut les fonctions d'authentification et de gestion des droits d'accès (sur la base des rôles – bien sûr !).

Souvent l'authentification peut être déléguée à un système de contrôle d'accès / SSO Web plus général. Il est à noter que dans ce cas de figure une configuration particulière est à mettre en place pour donner la possibilité d'accès aux pages de re-initialisation du mot de passe perdu à un utilisateur non authentifié.

7 - Aspects juridiques

Nous présentons dans ce chapitre plusieurs textes importants, français ou internationaux, qui contribuent à justifier la mise en œuvre d'un système de gestion des identités. Le point commun à ces textes récents est l'exigence de traçabilité, exigence qui ne saurait être satisfaite sans une identification efficace des utilisateurs des Systèmes d'Information.

Du fait que la gestion d'identités traite nécessairement certaines données nominatives, les textes relatifs à l'informatique et aux libertés revêtent également une importance particulière.

7.1. La loi Sarbanes-Oxley

Votée par le Congrès américain en juillet 2002 suite aux scandales ENRON et WORLDCOM, la loi Sarbanes-Oxley implique que les présidents des entreprises cotées aux États-Unis ou qui empruntent sur le marché des États-Unis et leurs filiales, y compris à l'étranger, certifient leurs comptes auprès de la Securities and Exchange Commission (SEC).

Elle est guidée par trois grands principes :

- exactitude et accessibilité de l'information,
- responsabilité des gestionnaires,
- indépendance des auditeurs.

La loi vise à augmenter la responsabilité des dirigeants et à mieux protéger les investisseurs. Elle a une portée extraterritoriale dans la mesure où les entreprises européennes doivent se soumettre à cette loi à partir du moment où elles sont cotées aux États-Unis. Les Systèmes d'Information sont impliqués :

- dans l'utilisation de l'informatique comme outil de gestion et de contrôle financier,
- dans l'obligation instituée d'assurer la sécurité de ce même système.

Le principal objectif est de renforcer le contrôle interne et de fournir des contrôles protégeant l'information contre toute utilisation, divulgation ou modification non autorisée, et contre tout dommage ou perte. Dans les Systèmes d'Information, cet objectif est atteint à l'aide de contrôle d'accès logique assurant l'accès aux systèmes, données et programmes aux seuls utilisateurs autorisés et à la traçabilité de ces accès. Cette activité de contrôle comporte 22 éléments différents, depuis les pare-feux jusqu'à la protection contre les virus et la réaction face à un incident en passant par la gestion, l'authentification et l'autorisation des utilisateurs.

7.2. La réforme Bâle 2

La réforme Bâle II du ratio de solvabilité bancaire s'inscrit dans une démarche mondiale de réglementation de la profession bancaire remontant à la fin des années 80, dont l'objectif premier est de prévenir les faillites.

Au delà de la dimension financière qui est le calcul des fonds propres à allouer, Bâle II prend en compte et place ses exigences sur les systèmes de notation et de surveillance. Bien plus, et c'est l'aspect le plus novateur, la réforme ne se limite plus aux seuls risques financiers « classiques », comme le risque de crédit ou les risques de marché (risque de change, risque de taux, etc.), mais couvre aussi le « Risque Opérationnel ».

Le Risque Opérationnel se définit comme le risque de pertes résultant de carences ou de défaillances attribuables à des procédures, personnels et systèmes internes ou à des événements extérieurs. Les Risques Opérationnels incluent notamment :

- les risques relatifs à la sécurité des biens et des personnes (incendie, inondation, tremblement de terre, attaque physique, sabotage, vol et fraude),
- les risques informatiques, liés aux développements et à la maintenance des programmes, aux traitements et à l'utilisation des services de télécommunications. Cette catégorie inclut en particulier le risque lié aux défauts de conception ou de réalisation d'une application, les incidents d'exploitation dans les systèmes de production, les accès non autorisés et les erreurs de traitement, ainsi que les pertes ou altérations accidentelles des données transmises et les défaillances dans la conservation de ces données,
- les risques de gestion interne, liés au fonctionnement interne de la banque, incluant les erreurs dans les traitements administratifs et comptables des opérations, les erreurs de conception ou de mise en place de nouveaux produits ou projets, la malveillance interne, les risques légaux, réglementaires ou déontologiques, les risques en matière de ressources humaines, de sous-traitance et de communication externe.

Les accords Bâle 2 conduisent à renforcer les contrôles de processus et à garantir la transparence dans les opérations financières. La gestion rigoureuse des identités et l'efficacité des contrôles d'accès contribuent de manière importante à ces objectifs.

7.3. La réforme Solvency 2

La réforme Solvency 2 pour les compagnies d'assurance est comparable à la réforme Bâle 2 pour les établissements financiers. Son objectif est de fournir un cadre d'évaluation de la solvabilité de ces établissements afin d'optimiser leurs fonds propres, sur la base de leurs risques réels et de critères qualitatifs.

L'entrée en vigueur de cette réforme est prévue sur 2010 – 2011.

7.4. Loi sur la Sécurité Financière – LSF

La loi n°2003-706 du 1er août 2003 de sécurité financière constitue la réponse du législateur français à la crise de confiance que connaissent les marchés financiers depuis le début des années 2000 suite aux scandales et aux faillites qui ont secoué les marchés.

Elle comporte des dispositions de nature financière mais également de nombreuses mesures intéressant les sociétés. Ces mesures tendent notamment à renforcer le contrôle des comptes et la transparence des entreprises.

La loi corrige ou adapte un certain nombre d'articles du code de commerce ou du code monétaire et financier.

7.5. Loi pour la confiance dans l'économie numérique – LEN ou LCEN

Cette loi du 21 juin 2004 a pour but de favoriser la confiance dans l'utilisation d'Internet en France. Elle aborde les principaux points suivants :

- la communication au public par voie électronique,
- la responsabilisation et les contraintes sur les pratiques commerciales,
- la réglementation envers les hébergeurs et les prestataires,
- l'équilibre entre les droits de l'expression et la garantie des droits de la personne,
- les dispositions relatives à la sphère publique et au développement des technologies de l'information et de la communication.

7.6. Loi organique des lois de finance – LOLF

La loi organique des lois de finances définit une nouvelle architecture du budget de l'état permettant un meilleur contrôle de son utilisation. La LOLF prévoit pour chaque action, la définition d'objectifs et d'indicateurs de contrôle et que chaque responsable rende des compte sur ses résultats.

Cette approche nécessite une révision des méthodes de travail et de nouvelles procédures associées à des exigences de traçabilité des opérations.

7.7. La norme IAS 39 (International Accounting Standards)

En juillet 2002, un règlement européen a entériné la décision de la Commission Européenne d'imposer à toutes les sociétés européennes cotées (y compris les banques et les sociétés d'assurance) l'élaboration de leurs états financiers consolidés conformément aux normes comptables IAS.

En norme comptable IAS, l'information financière ne repose plus sur la notion de coût historique mais celle de la « juste valeur ». L'application de ces normes et particulièrement l'IAS 39 doit permettre :

- Plus de transparence financière.
- Une comparabilité des états comptables
- Une amélioration de la qualité de l'information plus économique

L'application de la norme IAS39 va avoir des conséquences fortes sur les systèmes informatiques, principalement sur la protection et l'intégrité des données.

7.8. CNIL

La loi « informatique et libertés » du 6 février 1978 a marqué une étape importante en France, et même en Europe, en réglementant la création et l'utilisation de fichiers contenant des données nominatives. Cette loi définit des obligations de protection et de déclaration des données personnelles et de leurs traitements à la CNIL, Commission Nationale de l'Informatique et des Libertés.

La loi de 1978 a été enrichie par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Cette nouvelle loi attribue des pouvoirs de sanction à la CNIL.

8 - Annexes

8.1. Glossaire

Terme	Commentaire
Administrateur du Workflow	L'administrateur du workflow dispose des droits pour contrôler et valider le Workflow d'habilitation. Cet administrateur définit les demandeurs, les approuveurs et le séquencement du processus.
Administrateur système	L'administrateur système dispose des droits sur les ressources et les comptes du système. Il gère ces ressources et affecte les droits d'accès aux rôles.
Administrateur de mots de passe	L'administrateur de mot de passe fait partie du Help Desk et dispose des droits sur la gestion des crédentiels. Il peut réinitialiser ou confirmer la réinitialisation du mot de passe d'un utilisateur et prendre les dispositions de sécurité utiles en cas d'incident de sécurité (verrouillage de compte).
Approbateur Métier (Business approuver)	L'approbateur métier dispose des droits pour valider ou refuser la création ou la modification des comptes en fonction du profil de l'utilisateur concerné.
Approbateur technique	L'approbateur technique donne son accord final pour valider la cohérence globale et la compatibilité technique des droits accordés à un utilisateur sur les comptes lors de leur création ou de leur modification.
Auditeur	Contrôle le respect des procédures.
Authentifiant	Attribut utilisateur couplé à l'identifiant et dont la fourniture conjointe permet d'assurer le processus d'authentification. L'authentifiant peut être le mot de passe géré par l'utilisateur.
Authentification	Processus permettant de s'assurer de façon sûre de l'identité d'un utilisateur lors des demandes d'accès au Système d'Information.
Autorisation	L'autorisation d'accès est donnée au cas par cas à un utilisateur par une application en fonction des droits associés au rôle applicatif (ou par une ressource en fonction des privilèges).
Compte	A chaque personne peuvent être associés des comptes d'accès aux différents systèmes et applications. Le compte contient les données qui permettent d'y accéder (identifiant + mot de passe).
Crédentiel (Credential)	Couple formé par un identifiant et un mot de passe (ou un autre moyen de validation d'identité comme certificats etc.) permettant l'authentification d'un utilisateur. Voir authentifiant.
Droits applicatifs	Droits applicatifs déterminent les actions possibles dans une application. Exemple s : lecture, écriture validation d'un masque, requête en base, impression d'une fiche, etc.)
État	Il permet de stipuler dans quel état sont les rôles, personnes et comptes : actif, en cours d'initialisation ou suspendu.

Terme	Commentaire
Gestionnaires des ressources humaines internes et externes	Fournit les informations sur l'identité des utilisateurs lors des arrivées ou départ de personnel ou lors de changement d'affectation. Dans le cas du personnel interne, il s'agit de la DRH. Pour les intervenants externes, c'est en général le commanditaire de la prestation.
Habilitation	L'habilitation est une association entre un utilisateur et N profils fonctionnels (chaque profil regroupant M rôles applicatifs). In fine, l'habilitation correspond à un processus permettant d'accorder aux acteurs des droits sur des ressources. Les habilitations sont exprimées par « Qui a accès à quoi? ».
Identifiant	Attribut permettant de caractériser de façon unique et univoque un utilisateur au sein d'un Système d'Information.
Mot de passe (Password)	Le mot de passe est la partie du crédentiel qui n'est connu que de l'utilisateur. Le système doit avoir un droit de contrôle des mots de passe en fonction de la politique de sécurité développée dans l'entreprise.
Personne	Le concept de Personne permet de décrire une personne physique correspondant à une "entrée" dans l'annuaire et à laquelle sont rattachés plusieurs attributs. Voir Utilisateur.
Politique de mot de passe	La politique de mot de passe présente un ensemble de règles de gestion définis par l'administrateur de mots de passe : pour spécifier la restauration des mots de passe oubliés (généralement par l'emprunt d'un mot de passe temporaire standard), pour caractériser la taille minimale, la composition (caractères Spéciaux, chiffres, ..), la forme, la durée de validité, etc.
Preuves d'authentification	Voir crédentiels et authentifiant
Profil métier	Un ensemble des rôles applicatifs regroupé pour faciliter l'administration.
Propriétaire fonctionnel	Définit les politiques applicables à l'information (règles d'accès et d'attribution des droits aux données et traitements), et est informé des conditions d'application des règles d'accès.
Rôle applicatif	Le rôle applicatif est un ensemble des droits propres à une seule application. Par exemple : le droit d'usage d'un jeu d'écrans et de menus correspondant à une fonction dans l'application. Un rôle appartient à une seule application. L'application admet plusieurs rôles. À un instant donné un utilisateur n'a qu'un rôle actif dans cette application.
Utilisateurs	Désigne le personnel, les prestataires, les partenaires, et les clients d'entreprise qui, de par leur fonction, exercent une activité ayant vocation à leur permettre de bénéficier des applications et des ressources mises à disposition par l'entreprise. Voir « Personne ».

8.2. Acronyme

Terme	Commentaire
ACL	Access Control List « *liste de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe.* »
CNIL	Commission Nationale de l'Informatique et des Libertés « *autorité administrative indépendante française chargée de veiller à la protection des données personnelles et à la protection de la vie privée.* »
CRM	Gestion de la Relation Client en abrégé GRC, en anglais Customer Relationship Management ou CRM « *Logiciel qui permet de gérer les étapes d'une politique commerciale (prospection, vente, après-vente).* »
DAC	Discretionary Access Control « *moyens de limiter l'accès aux objets basés sur l'identité des personnes ou des groupes auxquels ils appartiennent.* »
DSD	Dynamic Separation of Duty Relations
DSML	Directory Services Markup Language
ERP	Progiciel de Gestion Intégré en abrégé PGI, en anglais Enterprise Resource Planning ou ERP « *Logiciel qui permet de gérer l'ensemble des processus d'une entreprise, en intégrant l'ensemble des fonctions de cette dernière comme la gestion des ressources humaines, la gestion comptable et financière, l'aide à la décision, mais aussi la vente, la distribution, l'approvisionnement, le commerce électronique.* »
FIM	Federated Identity Management
HTTPS	Hypertext Transfer Protocol Secured « *variante de HTTP basée sur les protocoles SSL ou TLS permettant au visiteur de vérifier l'identité du site auquel il accède grâce à un certificat d'authentification.* »
IAM	Identity Access Management
IDP	Identity Provider
IP	Internet Protocol « *protocole utilisé pour le routage des paquets sur les réseaux.* »
J2EE	Java 2 Platform, Enterprise Edition « Langage de programmation Java destinée aux applications d'entreprise. »
LDAP	Lightweight Directory Access Protocol « *protocole permettant l'interrogation et la modification des services d'annuaire reposant sur TCP/IP et respectant le modèle X.500.* »
MAC	Mandatory Access Control « *méthode de gestion des droits des utilisateurs pour l'usage de Systèmes d'Information.* »
MLS	Multi-Level Security

Terme	Commentaire
MOA	Maître D'Ouvrage ou Maîtrise D'Ouvrage « *représente une personne physique ou morale (entreprise, direction, etc.), responsable de la bonne compréhension et des bonnes relations entre les directions métier et les directions informatiques.* »
MOE	Maître d'Œuvre ou Maîtrise d'Œuvre « *représente une personne physique ou morale (entreprise, direction, etc.) garante de la bonne réalisation technique des solutions.* »
NOS	Network Operating System « *type de système d'exploitation* »
NSA	National Security Agency « *organisme gouvernemental des États-Unis, responsable de la collecte et de l'analyse de toutes formes de communications et de leur sécurité.* »
OASIS	Organization for the Advancement of Structured Information Standards
ODBC	Open DataBase Connectivity « *format permettant la communication entre des clients bases de données fonctionnant sous Windows et les SGBD.* »
OS	Operating System « *système d'exploitation en français.* »
PC	Personal Computer « *utilisé pour désigner un ordinateur personnel, par opposition aux ordinateurs de taille différentes (assistant personnel, station de travail, ordinateur central, superordinateur, etc.).* »
PDA	Personal Digital Assistant « *appareil numérique portable.* »
PKI	Public Key Infrastructure « *ensemble de composants physiques (ordinateurs, équipements cryptographiques, cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.* »
POC	Proof Of Concept « *réalisation courte et/ou incomplète d'une certaine méthode ou idée pour démontrer sa faisabilité.* »
RBAC	Role-Based Access Control « *modèle de contrôle d'accès à un Système d'Information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est attaché.* »
RSSI	Responsable de la Sécurité des Systèmes d'Information « *responsable du maintien du niveau de sécurité du Système d'Information.* »
SAML	Security Assertion Markup Language « *standard informatique définissant un protocole pour échanger des informations liées à la sécurité, basé sur le langage XML.* »
SGBD	Système de Gestion de Base de Données « *ensemble de programmes constituant la gestion et l'accès à plusieurs bases de données.* »

Terme	Commentaire
SI	Système d'Information « *représente l'ensemble des éléments participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein d'une organisation.* »
SP	Service Provider
SPML	Service Provisioning Markup Language
SSD	Static Separation of Duty Relations
SSL	Secure Socket Layer « *protocole de sécurisation des échanges sur Internet, Renommé en 2001 en TLS (Transport Layer Security).* »
SSO	Single Sign-On « *méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques.* »
TLS	Transport Layer Security *« protocole de sécurisation des échanges sur Internet. »*
URL	Uniform Resource Locator « *chaîne de caractères utilisée pour adresser les Ressources dans le World Wide Web : document HTML, image, son, forum Usenet, boîte aux lettres électronique, etc., informellement appelée une adresse Web.* »
USB	Universal Serial Bus « *bus informatique plug-and-play servant à brancher des périphériques informatiques à un ordinateur pour communiquer en série.* »
XML	Extensible Markup Language « *langage informatique de balisage générique.* »