IAM - Gestion des identités et des accès : concepts et états de l'art

Guillaume Harry

IAM :
GESTION DES IDENTITES ET DES ACCES
CONCEPTS ET ETATS DE L'ART

Référence : IAM - Gestion des identités et des accès : concepts et états de l'art

Date de dernière mise à jour : 09/10/2013

Version du document : 1.2

Etat : ~~en cours~~ – terminé – ~~validé~~

Auteurs : Guillaume HARRY

Objet du document :

Ce document décrit les concepts et les meilleures pratiques pour la gestion des identités et des accès.

TABLE DES MISES A JOUR DU DOCUMENT

Version du document	Date	Objet de la mise à jour
1.0	01/06/2013	Création du document
1.1	04/06/2013	Anonymisation des exemples
1.2	09/10/2013	Corrections

LISTE DES ABREVIATIONS

- ABAC : **A**ttribute **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle d'accès basé sur les attributs (français)
- ACL : **A**ccess **C**ontrol **L**ist (anglais)
  Liste de contrôle des accès (français)
- CIL : **C**orrespondant **I**nformatique et **L**ibertés
- CNIL : **C**ommission **N**ationale **I**nformatique et **L**ibertés
- CRBAC : **C**onstrained **R**ole **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle d'accès basé sur les rôles avec contraintes (français)
- CRBF : **C**omité de **R**églementation **B**ancaire et **F**inancière
- DAC : **D**iscretionary **A**ccess **C**ontrol (anglais)
  Contrôle d'accès discrétionnaires (français)
- HRBAC : **H**ierarchical **R**ole **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle d'accès basé sur les hiérarchies de rôles (français)
- IAM : **I**dentity & **A**ccess **M**anagement (anglais)
  Gestion des Identités et des Accès (français)
- IBAC : **I**dentity **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle des accès basé sur l'identité (français)
- IdP : **Id**entity **P**rovider (anglais)
  Fournisseur d'identité (français)
- IUP : **I**dentifiant **U**nique **P**ersonnel
- MAC : **M**andatory **A**ccess **C**ontrol (anglais)
  Contrôle d'accès obligatoire (français)
- NIST : **N**ational **I**nstitute of **S**tandards and **T**echnology
- PDCA : **P**lan **D**o **C**heck **A**ct/**A**djust (anglais)
  Planifier **D**éployer **C**ontrôler **A**gir/**A**juster (français)
- RBAC : **R**ole **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle d'accès base sur les rôles (français)
- RP : **R**elying **P**arty (anglais)
  Consommateur (français)
- SMSI **S**ystème de **M**anagement de la **S**écurité de l'**I**nformation
- SoD : **S**egregation **o**f **D**uty (anglais)
  Séparation des responsabilités (français)
- SOX : **S**arbanes-**Ox**ley
- SP : **S**ervice **P**rovider (anglais)
  Fournisseur de service (français)
- SSO : **S**ingle **S**ign-**O**n (anglais)
  Authentification unique (français)

SOMMAIRE

1. INTRODUCTION 1

2. GESTION DES IDENTITES 2

2.1 Définitions 2
2.1.1 Identité 2
2.1.2 Attributs et identifiants 2
2.1.3 Fournisseurs de service et d'identité 3
2.1.4 Fédération d'identité 4
2.1.5 Gestion des identités 4
2.1.6 Exemples 5
2.2 Modèles 7
2.2.1 Identité isolée 7
2.2.2 Identité fédérée 8
2.2.3 Identité centralisée 10
2.3 Cadre réglementaire 14

3. GESTION DES ACCES 16

3.1 Définitions 16
3.1.1 Ressources et gestion des accès 16
3.1.2 Comptes utilisateurs 16
3.1.3 Habilitations et contrôle d'accès 17
3.1.4 Rôle, profil, groupe et périmètre 17
3.1.5 Authentification et autorisation 19
3.1.6 Exemples 20
3.2 Modèles 21
3.2.1 Identity based access control (IBAC) 22
3.2.2 Mandatory Access Control (MAC) 22
3.2.3 Role Based Access Control (RBAC) 23
3.2.4 Attribute Based Access Control (ABAC) 25
3.2.5 Organization Based Access Control (OrBAC) 25
3.2.6 Comparaison 26
3.3 Cadre réglementaire 26
3.3.1 Loi américaine Sarbanes-Oxley 26
3.3.2 Accords internationaux Bâle II 27
3.3.3 Loi de sécurité financière (LSF) 28
3.3.4 CRBF 97-02 28

4. BONNES PRATIQUES 30

4.1 Normes 30
4.1.1 ISO-24760 30
4.1.2 ISO-2700x 30
4.2 Démarche projet orientée gestion des identités et des accès 32

5. GLOSSAIRE 34

6. BIBLIOGRAPHIE 36

6.1 Références documentaires 36
6.2 Références Internet 37

ANNEXE 1. ISO 24760 (TABLE DES MATIERES) 38

ANNEXE 2. ISO-27002 (TABLE DES MATIERES - CHAPITRE 11) 39

ANNEXE 3. GESTION DE PROJET 40

1. Cycle de vie 40
2. Cycle en cascade 41
3. Cycle en V 42
4. Cycle en spirale 44
5. Méthodes Agiles 46

ANNEXE 4. THE MANIFESTO FOR AGILE SOFTWARE DEVELOPMENT 48

ANNEXE 5. GRILLE D'EVALUATION TECHNIQUE 49

1. Gestion des identités 49
2. Gestion des accès 50

LISTE DES FIGURES

Figure 1 - Diagramme de classe du concept d'identité 2
Figure 2 – Diagramme de classe des concepts d'attribut et d'identifiant 3
Figure 3 - Cycle de vie d'une identité 5
Figure 4 – Modèle de gestion d'identité : « identité isolée » 7
Figure 5 - Modèle de gestion d'identité : « identité fédérée » 9
Figure 6 - Modèle de gestion d'identité : « identité commune » 11
Figure 7 - Modèle de gestion d'identité : « méta-identité » 12
Figure 8 - Modèle de gestion d'identité : « Single Sign-On » 13
Figure 9 - Diagramme de classe des comptes 17
Figure 10 - Diagramme de classe des habilitations 19
Figure 11 - Processus itératif PDCA de la norme ISO-27001 31
Figure 12 - Cycle de vie de projet en cascade 41
Figure 13 - Cycle de vie de projet en V 42
Figure 14 - Diagramme d'activité d'une démarche itérative 44
Figure 15 - Diagramme d'activité de réalisation d'un prototype 44
Figure 16 - Cycle de vie de projet en spirale 45
Figure 17 - Cycle de vie en « Agilité » 47

Liste des tableaux

Tableau I - Exemple d'identités 6
Tableau II - Exemple de services 6
Tableau III - Synthèse de l'exemple pour le modèle d'identité isolée 8
Tableau IV - Synthèse de l'exemple pour le modèle d'identité fédérée 10
Tableau V - Synthèse de l'exemple pour le modèle d'identité commune 11
Tableau VI - Synthèse de l'exemple pour le modèle de méta-identité 12
Tableau VII - Synthèse de l'exemple pour le modèle de Single Sign-On 13
Tableau VIII - Exemple de comptes utilisateurs 20
Tableau IX - Exemple de rôles applicatifs 21
Tableau X - Exemple de profils 21
Tableau XI - Exemple de matrice ACL du modèle IBAC 22
Tableau XII - Exemple d'implémentation du modèle MAC 23
Tableau XIII - Grille d'évaluation technique : Référentiel intégré 49
Tableau XIV - Grille d'évaluation technique : Connecteurs 49
Tableau XV - Grille d'évaluation technique : Transformation 49
Tableau XVI - Grille d'évaluation technique : Provisioning 50
Tableau XVII - Grille d'évaluation technique : Gestion des rôles 50
Tableau XVIII - Grille d'évaluation technique : Gestion des habilitations 50
Tableau XIX - Grille d'évaluation technique : Gestion des mots de passe 51
Tableau XX - Grille d'évaluation technique : Contrôle et traçabilité 51

1. Introduction

La notion d'équipe virtuelle ou d'entreprise virtuelle est née dans les années 1990 pour décrire les nouvelles formes de management et d'échanges numériques inter-équipes ou inter-entreprises. L'organisation virtuelle est définie comme « une alliance temporaire d'organisations (institutions, industries, entreprises, …) indépendantes, connectées, géographiquement disséminées, incluant un haut niveau de confiance qui collaborent et partagent leurs ressources et compétences dans le but de répondre aux demandes des clients » [1]. Ce nouveau schéma d'organisation a pour objectif de mener à bien un projet et prend fin quand la phase de production commence. Ainsi, l'équipe formée de l'ensemble des personnes impliquées dans les différentes phases, incluant les membres des maitrises d'ouvrage, des maitrises d'œuvre et des fournisseurs, peut être définie comme une organisation virtuelle.

Comme pour tout projet, le succès réside sur une relation de confiance autour du partage des connaissances et des compétences. La communication est donc un facteur clé de réussite de ce type particulier d'organisation où les distances et la dématérialisation sont une difficulté. En effet, toutes les personnes participantes doivent avoir accès aux informations et outils mis en commun au moment opportun.

La flexibilité est une autre caractéristique des organisations virtuelles. En effet, leur nature dynamique est due à la participation ponctuelle des membres. Les participants rejoignent et quittent le projet en fonction des compétences requises dans les différentes phases. La complexité se situe pour les coordinateurs dans la fourniture rapide d'un accès aux moyens mis en commun et dans la révocation de ces autorisations aussitôt après leur départ. Les responsables doivent également s'assurer que le savoir-faire acquis ainsi que les réalisations soient préservés et partagés même après la fin de la collaboration.

Les technologies de l'information et de la communication mis en œuvre ont alors pour objectif de mettre en relation les membres de l'équipe virtuelle et les systèmes d'informations des organisations physiques d'origine impliquées dans le partenariat. La difficulté réside alors dans les différences au niveau des infrastructures et des politiques de sécurités implémentées par chacun des partenaires. Chacun d'entre eux doit s'interconnecter avec les autres et permettre le partage des ressources tout en préservant la sécurité de sa propre organisation [2]. Tous doivent offrir un moyen de communication assurant l'intégrité et la confidentialité des données. De même, ils doivent disposer d'un moyen de vérifier l'identité des personnes et des systèmes qui prennent part dans la collaboration.

[1] M.R. Nami, A. Malekpour. Virtual Organizations : Trends and Models. Dans IFIP International Federation for Information Processing, Volume 288; *Intelligent Information Processing IV*; Zhongzhi Shi, E. Mercier-Laurent, D. Leake, p 190–199, 2008

[2] J. Magiera, A. Pawlak. Security Frameworks for virtual organizations. Dans *Organizations: Systems and Practices*. Springer, pages 133-148, 2005

2. Gestion des identités

2.1 Définitions

2.1.1 Identité

Dans l'article « Trust Requirements in Identity Management » [3], l'identité est définie comme « un ensemble de caractéristiques propres par lesquelles une personne ou une organisation est connue ou reconnue. Ces éléments peuvent être définis, comme le nom, l'adresse, la nationalité, ou peuvent être innés comme les empruntes digitales. Pour l'identité d'une organisation, les caractéristiques sont acquises ».
Le standard international ISO/IEC 24760-1[4], basé sur la recommandation UIT-T Y.2720 rédigée par l'Union Internationale des Télécommunications, étend la définition d'identité à l'« information utilisée pour représenter une entité dans un système d'information et de communication ». Une entité représente une personne physique ou morale (organisation, entreprise, …), une ressource (un objet tel qu'un matériel informatique, un système d'information ou de communication) ou un groupe d'entités individuelles.

Une entité peut posséder plusieurs identités numériques. Chaque identité permet alors d'exposer des informations en fonction de l'environnement. Ainsi, un individu peut présenter, par exemple, des informations publiques le concernant dans le cadre de son activité professionnelle, ce qui représentera une identité, et d'autres informations personnelles le présentant dans son contexte familial, ce qui désignera une autre identité.

Une identité peut être utilisée dans plusieurs contextes. Conjointement, dans un même domaine, une entité peut être incarnée par plusieurs identités. De plus, plusieurs identités d'une même entité peuvent partager les mêmes caractéristiques, ce qui implique que les identités peuvent ne pas être uniques dans un même contexte.

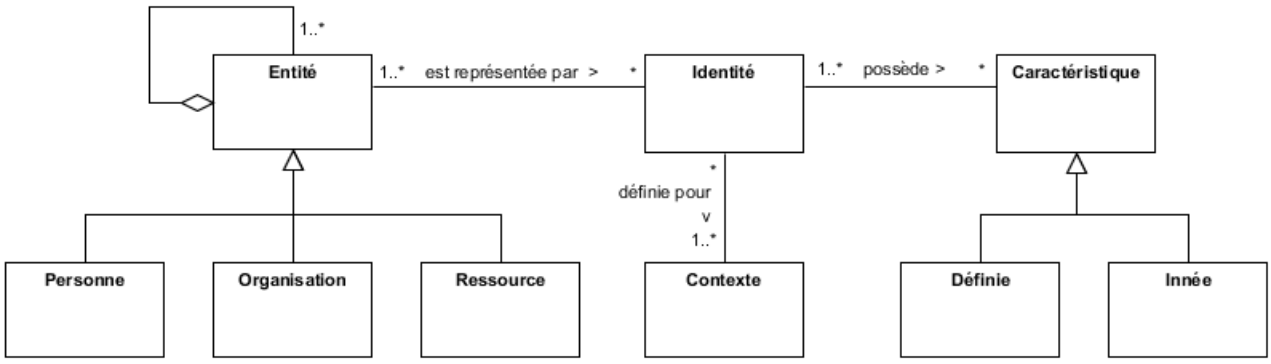

Figure 1 - Diagramme de classe du concept d'identité

Dans le présent document, le terme d'identité fera référence à une identité numérique limitée aux informations utilisées dans le contexte professionnel dont l'employeur doit gérer le cycle de vie.

2.1.2 Attributs et identifiants

L'attribut d'une identité décrit une caractéristique d'une entité dans un contexte déterminé [4]. Chaque attribut est défini par un type, une valeur et un contexte. Il peut éventuellement avoir un nom qui peut être utilisé pour le référencer. Un attribut certifié

[3] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope. Trust Requirements in Identity Management. *Australasian Information Security Workshop 2005* volume 44, pages 99-108, 2005

[4] ISO/IEC 24760-1:2011(E). ISO/IEC, 20 pages, 2011

conforme par un organisme officiel et/ou digne de confiance est appelé « claim » (la traduction française étant « affirmation »).

L'identifiant est une information qui permet de distinguer sans ambiguïté une identité d'une autre pour un contexte donné. L'identifiant peut être un attribut. Dans ce cas, la valeur d'un identifiant ne peut pas être utilisée par plusieurs identités. De ce fait, il est généralement utilisé dans le processus d'identification qui est responsable de la reconnaissance de l'identité dans un contexte. De même qu'une entité peut posséder plusieurs identités pour présenter des informations en fonction des contextes, une identité peut être représentée par plusieurs identifiants.

L'identifiant de référence est un identifiant pour un contexte donné qui ne changera pas pendant la durée de vie de l'entité qu'elle représente. Il doit perdurer tant que l'entité doit être connue du domaine. Il peut même durer plus longtemps, en fonction de la politique d'archivage à laquelle est soumise l'organisation. L'identifiant de référence ne pourra être utilisé par une autre entité uniquement sous condition que l'entité propriétaire ne soit plus référencée dans le domaine et après une période déterminée par la politique de sécurité du domaine.

L'identifiant unique personnel (IUP) est un identifiant qui permet de désigner une entité. Sa valeur est donc la même pour les toutes les identités d'une même entité. Deux entités ne peuvent pas partager le même identifiant unique personnel.

Les justificatifs d'identité (en anglais : « identity credentials ») sont des informations qui peuvent être utilisées en tant qu'attestation de l'identité revendiquée par une entité. Il peut s'agir d'une chaîne de caractère connue uniquement de l'identité (mot de passe) ou d'une empreinte digitale par exemple.

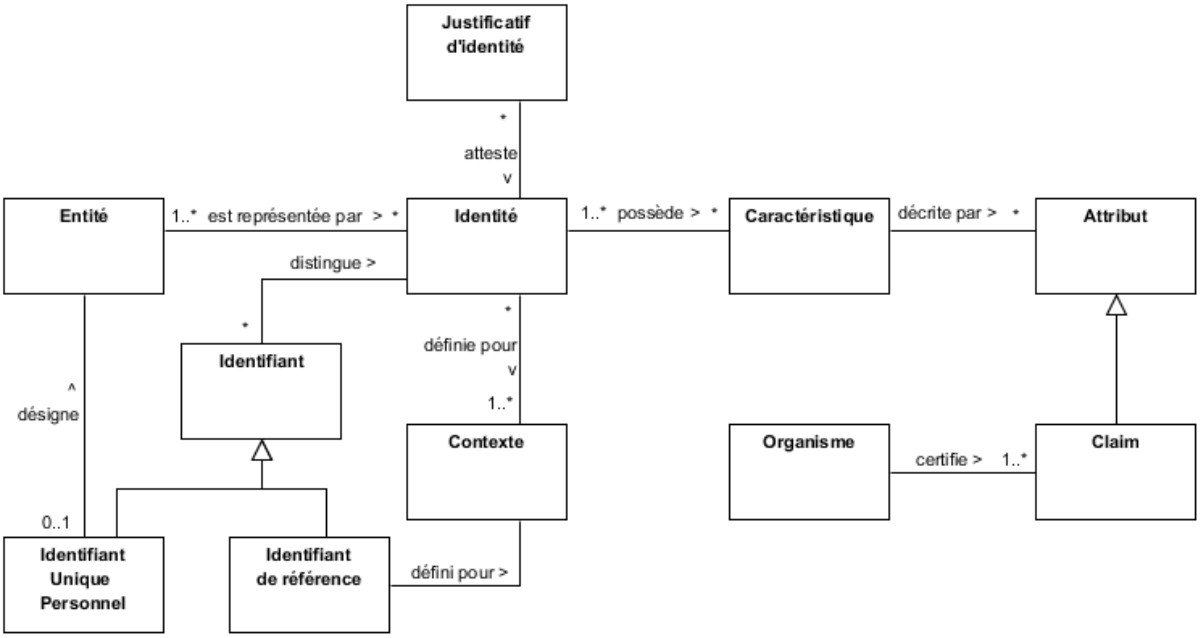

Figure 2 – Diagramme de classe des concepts d'attribut et d'identifiant

2.1.3 Fournisseurs de service et d'identité

Le fournisseur de service (SP : « Service provider » en anglais) est une ressource informatique qui est le support à la réalisation d'une activité d'une organisation (réelle ou virtuelle). Un fournisseur de service peut être un système d'information de gestion ou le système qui pilote une machine à commande numérique. Dans certains cas, l'accès au service

est restreint et l'identité des utilisateurs doit être vérifiée avant de pouvoir lancer l'exécution d'une tâche.

Le fournisseur d'identité (IdP : « Identity provider » en anglais) est un fournisseur de service qui construit la représentation numérique des identités [5]. Il est notamment responsable de la gestion des attributs et le garant de l'alimentation de leurs valeurs.

Un fournisseur de service peut être mis en œuvre en corrélation avec le fournisseur d'identité afin de gérer les aspects liés à l'authentification (processus de vérification de l'exactitude d'un ou plusieurs attributs d'une identité) pour les autres fournisseurs de service de l'organisation. Dans ce cas, ce fournisseur de service est un support à la notion de confiance évoquée pour les organisations virtuelles et à la politique de sécurité de l'organisation.

Le consommateur d'identité (RP : « Relying Party » en anglais) est un fournisseur de service dont l'utilisation nécessite l'authentification des identités présentées par un fournisseur d'identité. En fonction du domaine d'activité de l'organisation et du type de service rendu, un consommateur d'identité peut être soumis au respect d'une ou plusieurs lois (cf. les paragraphes « Cadre juridique » des chapitres « Gestion des identités » et « Gestion des accès »). Dans ce cas, l'organisation est contrainte à la mise en place d'outils de contrôles et de gestion des processus liés aux identités.

Un domaine d'identité correspond à l'ensemble composé d'un fournisseur d'identités et des consommateurs d'identités pour lesquels une identité est connue et utilisable. Le concept de « contexte » évoqué précédemment peut être un domaine d'identité.

2.1.4 Fédération d'identité

Une fédération d'identité est un accord entre plusieurs domaines d'identités qui spécifie comment les différentes parties prenantes peuvent échanger des informations relatives aux identités. L'accord définit les protocoles utilisés, les formats des données et les procédures de protection et d'audit. L'identité ainsi fédérée pourra être utilisée dans les différents domaines de la fédération.

2.1.5 Gestion des identités

Le CLUSIF [6] définit la gestion des identités comme la gestion du « cycle de vie des personnes (embauche, promotion, mutation, départ, etc.) au sein de la société et les impacts induits sur le système d'information ». Ces changements ont des conséquences sur les informations connues et gérées par le domaine d'identité de l'organisation.

En effet, avant de travailler au sein d'une équipe, une relation contractuelle est établie avec la personne, que ce soit directement pour ce qui concerne un employé, par l'intermédiaire d'un partenaire ou par l'intermédiaire d'une société de service pour un prestataire. Ce contrat définit la mission de l'individu qui inclut des informations telles que le résultat attendu, la date de début de mission et sa durée. En contre partie du travail fourni, l'organisation s'engage à rémunérer l'individu directement ou via son organisation d'appartenance, selon le type de relation établie. Le contrat permet également d'initier les démarches administratives telles que l'enregistrement auprès du service de comptabilité qui initiera le processus de paiement de la paie ou de la facture. Il est également le socle qui

[5] E. Bertino, K. Takahashi. *Identity Management: Concepts, technologies and systems*. Artech House, 194 pages, 2010

[6] A. Balat, R. Bergeron, A. Butel, M. Cottreau, F. Depierre, G. Khouberman, L. Mourer, W. Poloczanski. *Gestion des identités*. CLUSIF, 63 pages, 2007

permet de mettre fin au processus de paiement. A partir de ces informations, une identité peut être construite puis enregistrée auprès du fournisseur d'identité.
Ensuite, lorsque la personne commence son contrat, l'identité qu'il doit présenter auprès des fournisseurs de service est activée, afin de lui permettre d'interagir avec les ressources utiles à sa mission.
A la fin de ladite mission, l'identité peut être suspendue, donc temporairement inutilisable, s'il est prévu de la réutiliser pour un prolongement de contrat par exemple. Une autre possibilité consiste à archiver l'identité. Cela implique que les informations lui étant liées ne sont plus exploitables pour l'authentifier auprès du domaine. Par contre, l'ensemble, ou une sous-partie, des informations archivées peut être réutilisé pour construire une nouvelle identité (processus de restauration).
Après un délai établi par l'organisation et par la loi, toutes les informations relatives à l'identité sont supprimées (cf. chapitre « Cadre réglementaire »).

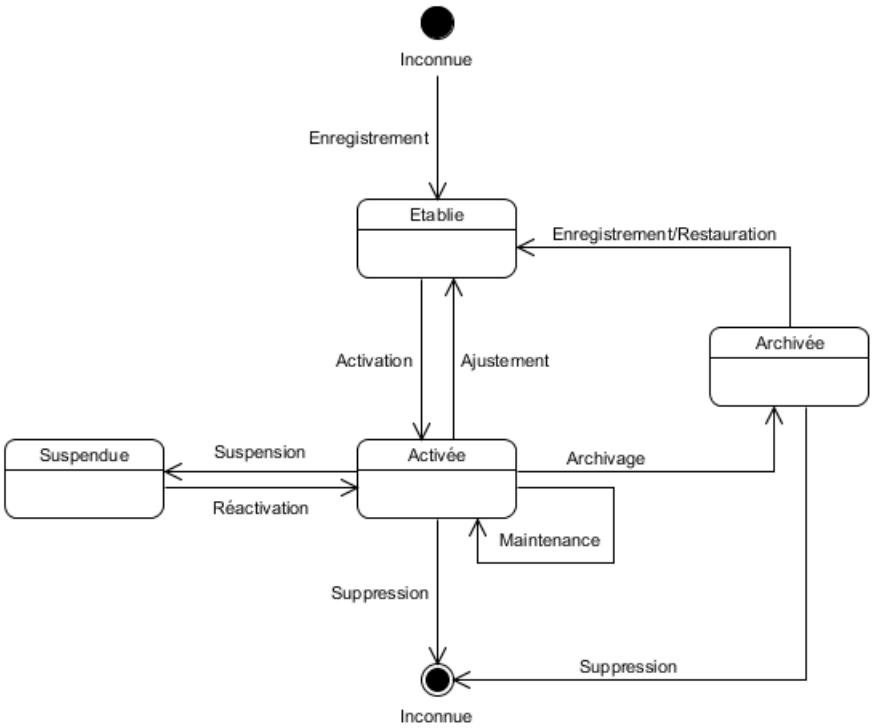

Figure 3 - Cycle de vie d'une identité

De plus, selon la norme ISO/IEC 24760 [4], la gestion des identités inclut la gouvernance, les politiques, les processus, les données, les technologies et les standards permettant notamment :

- d'authentifier les identités,
- d'établir la provenance des informations des identités,
- d'établir le lien entre les informations sur les identités et les entités,
- de maintenir à jour les informations sur les identités,
- d'assurer l'intégrité des informations sur les identités,
- de fournir les justificatifs d'identité et les services pour faciliter l'authentification d'une entité en tant qu'identité reconnue,
- d'ajuster les risques de sécurité liés au vol d'information par exemple.

2.1.6 Exemples

Une personne travaillant pour une organisation peut être connue sous plusieurs identités. Ce cas de figure se présente notamment lorsque la personne travaille pour plusieurs pôles ou

occupe différentes fonctions. En effet, dans le contexte de l'activité d'ingénieur qu'une personne exerce au sein d'un département, son organisation le connaît par exemple sous l'identité « Ingénieur CNRS *Jean Perrin* du département *uuu* ». Parallèlement, il peut être chargé d'une mission d'encadrement dans un autre département. Dans ce cas, l'établissement lui fournit et gère l'identité « Manager du département *xxx J.B. Perrin* ». Conjointement à ces activités, en tant qu'employé, son employeur produit l'identité « Employé *Jean-Baptiste Perrin* ». Ces identités ne sont valables que pour le contexte « *Entreprise* ». Dans le cas où l'entreprise est une des filiales d'un groupe, ces identités pourraient ne pas être connues des autres filiales du groupe, selon que le contexte soit fixé au niveau du groupe ou de la filiale.

Les caractéristiques appartenant à chaque identité ne sont pas nécessairement communes et les attributs les présentant sont construits indépendamment. Par ailleurs, les identités ne sont pas obligatoirement liées. Ainsi, les identités « Ingénieur » et « Manager » peuvent être liées à l'identité « Employé » permettant à cette dernière d'avoir accès à certaines informations des autres identités. Inversement, les deux premières identités sont indépendantes et n'ont pas de visibilité sur les informations d'autres identités.

Tableau I - Exemple d'identités

	Ingénieur	**Manager**	**Employé**
Nom	PERRIN	PERRIN	PERRIN
Prénom	Jean	J.B.	Jean-Baptiste
Date de naissance	30 septembre	30 septembre	30 septembre
Lieu de naissance	-	-	LYON
Diplômes	-	-	Agrégation de physique Doctorat ès sciences physiques
Quotité de travail	50%	50%	100%
Affectation	Département *uuu*	Département *xxx*	-
Employeur			
Identifiant	jean-baptiste.perrin	JBP	153545
Justificatif d'identité	Certificat numérique	« @zer1yuioP »	« azertyuiop »

L'organisation met à disposition un service de compte-rendu d'activité, un service de dépôt et consultation de documents techniques pour les ingénieurs, un service de gestion des congés, un service d'accès au dossier pour la retraite pour les employés, un service de saisie des demandes de moyens pour le service et un service de gestion du budget du département à destination des responsables de département.

Tableau II - Exemple de services

Service	**Identité utilisatrice potentielle**
Compte-rendu de l'activité (Crac)	Ingénieur
Dépôt et consultation de documents techniques (Doc)	Ingénieur
Gestion du budget du service (Bdg)	Manager
Saisie des demandes de moyens (Ddm)	Manager
Dossier de retraite (Ret)	Employé
Gestion des congés (Cge)	Employé

2.2 Modèles

Dans un domaine d'identité, le partage des attributs utilisés par les mécanismes d'identification (association de l'identifiant et d'un justificatif d'identité ; l'identification est souvent réalisée conjointement à l'authentification) implique pour les fournisseurs de service de partager les risques en cas de corruption d'une identité. Les différents modèles de gestion des données permettent donc de déporter les risques et les charges d'administration à différents niveaux. Différents modèles de gestion des identités peuvent cohabiter au sein de la même organisation. A. Jøsang, J. Fabre, B. Hay, J. Dalziel et S. Pope [3] proposent les trois modèles suivants de gestion des identités.

2.2.1 Identité isolée

Dans ce modèle, chaque fournisseur de service utilise son propre domaine d'identité, donc, son propre fournisseur d'identité. Un utilisateur doit utiliser un identifiant et un justificatif d'identité différents pour s'authentifier auprès de chacun des domaines.

Du point de vue de chacun des fournisseurs d'identité, la gestion des identités est plus simple. De plus, en cas de corruption d'identité dans un domaine d'identité, les autres fournisseurs de service ne sont pas impactés. Ce modèle a également l'avantage de permettre de définir un niveau de sécurité différent pour les justificatifs d'identités (longueur du mot de passe, nombre de justificatifs à présentés, etc.).

Cependant, cette approche peut devenir complexe du point de vue de l'utilisateur. En effet, ce dernier doit répéter les étapes d'authentification et d'identification auprès de chacun des domaines d'identité rattachés aux fournisseurs de services. De ce fait, il doit gérer et se souvenir d'autant d'identifiants et d'informations utiles à l'authentification que de services auxquels il doit accéder. Cela augmente donc le risque d'oubli ou de perte de ces informations, surtout pour les services auxquels il n'accède que rarement. De plus, cette situation peut être source de faible adhérence à la politique de sécurité de l'organisation qui sera jugée trop contraignante.

Le schéma ci-dessous représente l'accroissement du nombre de domaines d'identité et par conséquent du volume d'information nécessaire en fonction du nombre de fournisseurs de services.

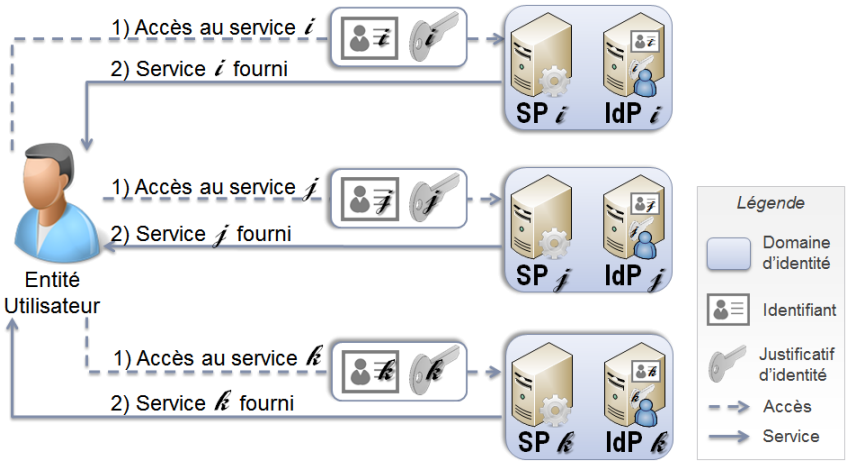

Figure 4 – Modèle de gestion d'identité : « identité isolée »

Dans le cadre de l'exemple décrit précédemment, l'utilisation du modèle d'identité isolée implique que chaque service que la personne doit utiliser correspond à un contexte unique. De ce fait, elle doit manipuler autant d'identités que de services. Ainsi, pour le service de gestion des congés, la personne présente l'identité « Employé - *Congés* » pour le domaine

d'identité « *Congés* », qui est un dérivé de l'identité « Employé CNRS » décrite précédemment. Ce contexte ayant son propre fournisseur d'identité, il doit gérer le cycle de vie de cette identité, ce qui inclut la mise à jour des informations, dont le justificatif d'identité et la génération d'un ou plusieurs identifiants. Pour utiliser les cinq autres services décrits précédemment, la personne doit présenter cinq autres identités distinctes potentiellement dissemblables. En effet, les fournisseurs d'identité peuvent utiliser des informations proches mais pourtant différentes. Les informations sont donc répliquées proportionnellement au nombre de services les utilisant. Cela augmente le risque d'erreur due à une rupture dans la chaîne d'approvisionnement. De plus, cette situation est aggravée par le cycle de mise à jour des informations et de renouvellement des justificatifs. Ces derniers sont gérés par des fournisseurs d'identités indépendants qui forcent ainsi l'utilisation de six justificatifs différents dans le cadre de l'exemple comme illustré dans le tableau suivant. En effet, les consommateurs d'identités peuvent demander des contraintes différentes sur les justificatifs d'identité. Par exemple, pour les mots de passe, la chaîne de caractère doit contenir un nombre minimum de caractères, de chiffres, de symboles ou non en fonction de la politique de sécurité du fournisseur de service.

Tableau III - Synthèse de l'exemple pour le modèle d'identité isolée

Fournisseur de service	**SP Crac**	**SP Doc**	**SP Bdg**	**SP Ddm**	**SP Ret**	**SP Cge**
Domaine d'identité	Crac	Doc	Bdg	Ddm	Ret	Cge
Fournisseur d'identité	IdP Crac	IdP Doc	IdP Bdg	IdP Ddm	IdP Ret	IdP Cge
Nom	PERRIN	PERRIN	PERRIN	PERRIN	PERRIN	P
Prénom	Jean	Jean-Baptiste	J.B.		Jean-Baptiste	JB
Affectation	Dept *uuu*	Dept *uuu*	Dept *xxx*	Dept *xxx*	-	-
Identifiant fourni et utilisé	jean.perrin @*uuu*.cnrs.fr	jb.perrin @*uuu*.cnrs.fr	jean.perrin @*xxx*.cnrs.fr	j-b.perrin @xxx.cnrs.fr	153545	JPB
Justificatif d'identité fourni et utilisé	Certificat numérique *uuu*.cnrs.fr	« azertyuio »	« @zer1yui0 »	Certificat numérique *xxx*.cnrs.fr	« Je@nPerr1n »	« JPB »

2.2.2 Identité fédérée

Dans l'article « Trust Requirements in Identity Management » [3], la fédération d'identité est définie comme un ensemble d'accords, standards et technologies permettant à un groupe de fournisseurs de service de reconnaître les identifiants provenant d'autres fournisseurs de services appartenant à la fédération. La fédération donne aux utilisateurs l'illusion de n'utiliser qu'un seul et unique identifiant alors qu'il continue à en présenter un différent à chaque fournisseur de service.

Dans une architecture d'identité fédérée, chaque fournisseur de service utilise son propre fournisseur d'identité, mais est capable d'accepter les identités provenant d'autres fournisseurs. L'accès à un fournisseur de service peut alors se faire au travers d'une identité d'un fournisseur d'identité autre que le sien. Comme pour le modèle isolé, une personne est connue par une identité par service au minimum, mais cette personne n'a pas à toutes les utiliser. Une correspondance est établie entre les identifiants des identités appartenant au même utilisateur dans le domaine d'identité fédéré. Quand un utilisateur est authentifié auprès

d'un premier fournisseur de service en utilisant un de ses identifiants et le justificatif qui lui est associé, tous les identifiants sont alors reconnus auprès de l'ensemble des fournisseurs d'identités de la fédération. Pour accéder à un autre fournisseur de service, l'utilisateur n'est alors pas soumis directement aux processus d'authentification et d'identification, car les informations sous-jacentes ont été transmises.

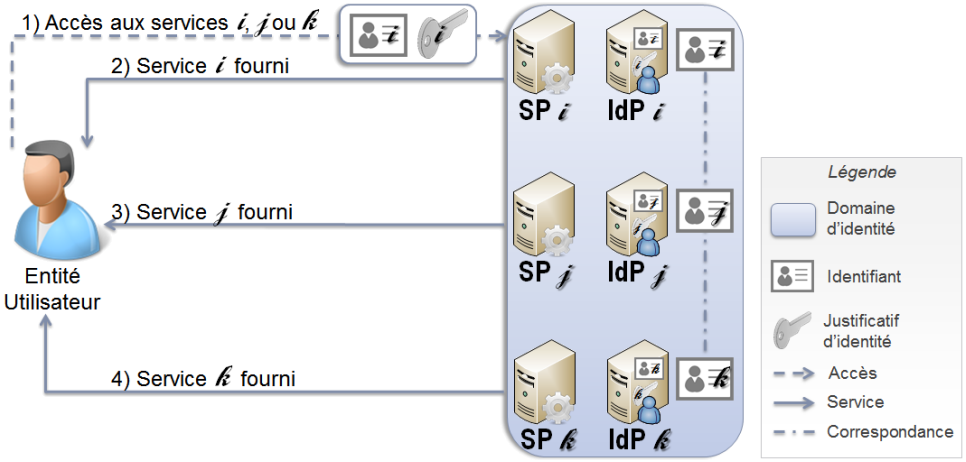

Figure 5 - Modèle de gestion d'identité : « identité fédérée »

Ce schéma illustre les avantages de la fédération pour l'utilisateur par rapport au modèle de gestion précédent, où chaque fournisseur de service utilisait indépendamment son propre domaine d'identité. En employant une identité fédérée, du point de vue de l'utilisateur, les informations nécessaires aux processus d'authentification et d'identification sont les mêmes quelques soient les fournisseurs de services sollicités. Il existe donc autant de domaines d'identité, de fournisseurs d'identité, d'identités que de services, mais l'utilisateur n'en n'a pas conscience.

Dans le cadre de l'exemple décrit précédemment, le modèle d'identité fédérée permet d'utiliser un unique couple identifiant-justificatif d'identité quel que soit le service demandé au sein d'une même fédération. Ainsi, l'organisation peut déployer une fédération « Ingénieur » pour l'ensemble des services liés aux activités d'ingénieur. Dans ce cas, la personne ne manipule qu'un seul couple identifiant-justificatif d'identité (« jean.perrin@*uuu*.cnrs.fr » - Certificat numérique « *uuu*.cnrs.fr »). L'identité correspondante (« Ingénieur - *Crac* ») est alors certifiée par le fournisseur d'identité « Crac » et de ce fait automatiquement acceptée par les autres fournisseurs d'identité de la fédération. Ensuite, une équivalence est établie par le fournisseur d'identité impactés « Doc », permettant de présenter l'identité « Ingénieur - *Doc* » au service « Doc ».
Une autre fédération « Manager » peut être mise en place pour les services mis à disposition des responsables de département. Dans ce cas, l'identifiant « j-b.perrin@*xxx*.cnrs.fr » assorti du certificat numérique « *xxx*.cnrs.fr » peut permettre d'utiliser le service de gestion du budget du département sous l'identité « Manager - *Bdg* » et le service de saisie des demandes de moyen sous l'identité « Manager - *Ddm* ». De même, une fédération peut être mise en place pour simplifier l'utilisation des services mis à disposition pour la gestion des ressources humaines.
Par contre, aucune interaction n'est possible nativement entre les différentes fédérations. Seule une fédération de fédération peut permettre d'établir des correspondances entre les domaines d'identité.

Tableau IV - Synthèse de l'exemple pour le modèle d'identité fédérée

Fournisseur de service	**Crac**	**Doc**	**Bdg**	**Ddm**	**Ret**	**Cge**
Domaine d'identité	Ingénieur		Manager		RH	
Fournisseur d'identité	IdP Crac	IdP Doc	IdP Bdg	IdP Ddm	IdP Ret	IdP Cge
Nom	PERRIN	PERRIN	PERRIN	PERRIN	PERRIN	P
Prénom	Jean	Jean-Baptiste	J.B.		Jean-Baptiste	JB
Affectation	Dept *uuu*	Dept *uuu*	Dept *xxx*	Dept *xxx*	-	-
Identifiant fourni	jean.perrin @*uuu*.cnrs.fr	jb.perrin @*uuu*.cnrs.fr	jean.perrin @*xxx*.cnrs.fr	j-b.perrin @xxx.cnrs.fr	153545	JPB
Justificatif d'identité fourni	Certificat numérique *uuu*.cnrs.fr	« azertyuio »	« @zer1yui0 »	Certificat numérique *xxx*.cnrs.fr	« Je@nPerr1n »	« JPB »
Identifiant utilisé	jean.perrin@*uuu*.cnrs.fr		j-b.perrin@*xxx*.cnrs.fr		153545	
Justificatif d'identité utilisé	Certificat numérique *uuu*.cnrs.fr		Certificat numérique *xxx*.cnrs.fr		« Je@nPerr1n »	

2.2.3 Identité centralisée

Dans ce modèle, seuls un identifiant et un justificatif sont utilisés par les fournisseurs de service. A. Jøsang, J. Fabre, B. Hay, J. Dalziel et S. Pope [3] donnent trois exemples d'implémentation de ce type de gestion d'identité.

- **Identité commune**

Dans ce modèle, une entité unique agit en tant que fournisseur d'identité pour l'ensemble des fournisseurs de service. Le mode de fonctionnement est à mi-chemin entre le modèle d'identité isolée et le modèle d'identité fédérée du point de vue de l'utilisateur. En effet, ce dernier doit répéter les processus d'authentification et d'identification avant de pouvoir utiliser un service. Cependant, le domaine d'identité rattaché à chacun des fournisseurs de service est le même. De ce fait, l'utilisateur utilise les mêmes informations d'identifiant et de justificatif quel que soit le fournisseur de service sollicité, ce qui simplifie l'accès aux différents services.

Avec ce type d'implémentation le fournisseur d'identité unique est un point central et sensible pour l'ensemble des fournisseurs de service. En effet, en cas de défaillance ou de modification au niveau du domaine d'identité, toutes les entités dépendantes sont impactées. De ce fait, ce modèle de gestion impose que chaque fournisseur de service lié au domaine d'identité unique soit déclaré explicitement. Dans le cas contraire, il est difficile d'évaluer les conséquences d'un changement ou d'une altération vis-à-vis des services mis à disposition de l'utilisateur par le biais de cette architecture.

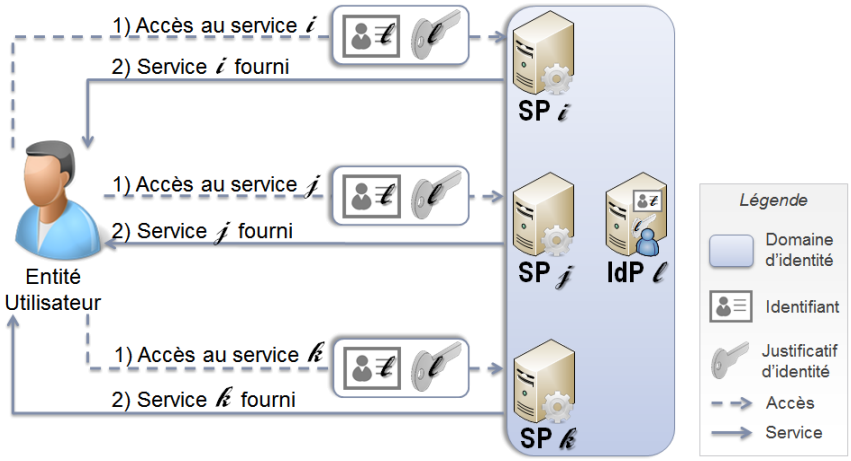

Figure 6 - Modèle de gestion d'identité : « identité commune »

Dans le cadre de l'exemple décrit précédemment, le modèle d'identité commune permet d'utiliser un unique couple identifiant-justificatif d'identité quel que soit le service demandé, comme dans le modèle d'identité fédérée. De ce fait, une seule identité est présentée aux différents services du domaine « RH ». L'unique fournisseur d'identité doit donc construire une identité qui contient les informations nécessaires aux différents services. Un protocole d'accord doit donc être accepté par les différents fournisseurs concernant le contenu et la forme des informations. Ainsi l'identité « Employé » doit contenir l'identifiant « 153545 » connu par le service « Ret » ainsi que l'identifiant « JPB » connu par le service « Cge ». Par contre les deux services doivent être capables de reconnaître le justificatif d'identité « Je@nPerr1n ». De même, dans les exemples précédents, les valeurs de l'attribut « prénom » des identités « Employé - *Ret* » et « Employé - *Cge* » n'étaient pas équivalentes, alors que le modèle d'identité commune impose que cet attribut soit partagé.

Tableau V - Synthèse de l'exemple pour le modèle d'identité commune

Fournisseur de service	**Crac**	**Doc**	**Bdg**	**Ddm**	**Ret**	**Cge**
Domaine d'identité	Ingénieur		Manager		RH	
Fournisseur d'identité	IdP Chercheur		IdP DU		IdP RH	
Nom	PERRIN		PERRIN		PERRIN	
Prénom	Jean-Baptiste		J.B.		Jean-Baptiste	
Affectation	Département *uuu*		Département *xxx*		-	
Identifiant applicatif 1	jean.perrin@*uuu*.cnrs.fr		jean.perrin@*xxx*.cnrs.fr		153545	
Identifiant applicatif 2	jb.perrin @*uuu*.cnrs.fr		j-b.perrin @*xxx*.cnrs.fr		JPB	
Identifiant utilisé	jean.perrin@*uuu*.cnrs.fr		j-b.perrin@*xxx*.cnrs.fr		153545	
Justificatif d'identité utilisé	Certificat numérique *uuu*.cnrs.fr		Certificat numérique *xxx*.cnrs.fr		« Je@nPerr1n »	

- **Méta-identité**

La mise en œuvre d'un domaine de méta-identité permet aux fournisseurs de service de partager des informations relatives aux identités. Par exemple, une correspondance peut être

établie entre les identifiants des différents domaines d'identité et un méta-identifiant (identifiant du domaine de méta-identité) qui n'est pas connu de l'utilisateur. Cet identifiant particulier permettant de désigner de façon unique une entité quelques soient les identités dans les domaines concernés, la notion de méta-identifiant se rapproche de la notion d'identifiant unique personnel.

Les justificatifs peuvent être liés au méta-identifiant. Dans ce cas, les justificatifs sont les mêmes pour tous les domaines d'identités concernés. Du point de vue de l'utilisateur, cette architecture peut être perçue comme un mécanisme de synchronisation des justificatifs entre les différents domaines d'identité.

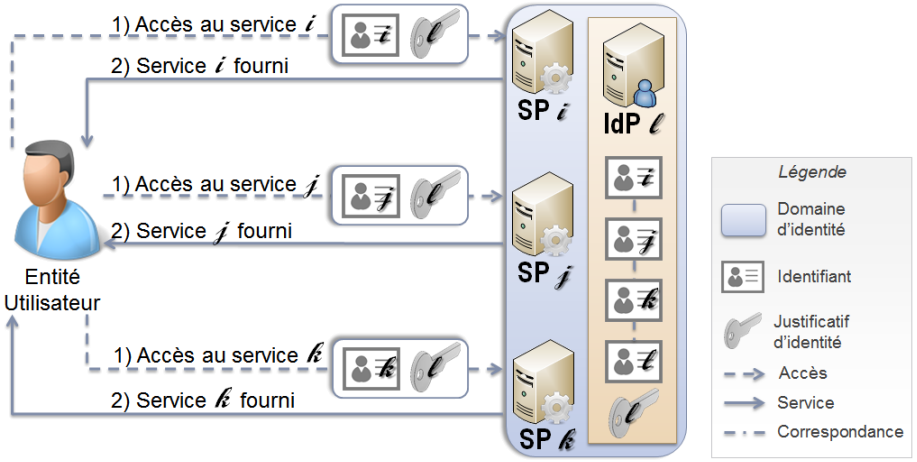

Figure 7 - Modèle de gestion d'identité : « méta-identité »

Cette approche est un moyen de faciliter l'intégration de différents domaines d'identité, comme lors de la fusion de plusieurs organisations. Ainsi, le modèle de méta-identité permet à des domaines d'identité isolés de mettre en commun des informations et éviter la réplication des informations. Dans le cadre de l'exemple d'identité isolée décrit précédemment, la mise en œuvre d'un domaine de méta-identité « Ingénieur » permet d'unifier les informations fournies par les fournisseurs d'identité « Crac » et « Doc ». La gestion de ces informations est alors déléguée au fournisseur de méta-identité « Ingénieur ». Par ailleurs, le fournisseur de service « Crac » doit être capable d'établir une correspondance entre l'identifiant fourni « jean.perrin@uuu.cnrs.fr » et le méta-identifiant « fsd15f7s51f2s74 » afin de pouvoir accepter le justificatif d'identité sous forme de certificat numérique. De même, le fournisseur de service « Doc » doit pouvoir faire le lien entre l'identifiant fourni « jb.perrin@uuu.cnrs.fr » et le méta-identifiant « fsd15f7s51f2s74 ». Pour l'ingénieur, le domaine de méta-identité permet de gérer moins de justificatifs d'identité. Cependant, contrairement aux modèles d'identité fédérée ou commune, la personne doit continuer à utiliser des identifiants différents. Cette architecture permet de restreindre le volume de données, mais la difficulté est de mettre en place un mécanisme qui permet de lier les informations gérées par le fournisseur d'identité « Crac » à celles du fournisseur d'identité « Doc ».

Tableau VI - Synthèse de l'exemple pour le modèle de méta-identité

Fournisseur de service	**Crac**	**Doc**	**Bdg**	**Ddm**	**Ret**	**Cge**
Domaine d'identité	Crac	Doc	Bdg	Ddm	Ret	Cge
Fournisseur d'identité	IdP Crac	IdP Doc	IdP Bdg	IdP Ddm	IdP Ret	IdP Cge
Nom	PERRIN		PERRIN		PERRIN	PERRIN

Fournisseur de service	Crac	Doc	Bdg	Ddm	Ret	Cge
Prénom	Jean-Baptiste		J.B.		Jean-Baptiste	JB
Affectation	Département *uuu*		Département *xxx*		-	
Identifiant fourni	jean.perrin @*uuu*.cnrs.fr	jb.perrin @*uuu*.cnrs.fr	jean.perrin @*xxx*.cnrs.fr	j-b.perrin @xxx.cnrs.fr	153545	JPB
Domaine de méta-identité	Ingénieur		Manager		RH	
Méta-identifiant	fsd15f7s51f2s74		dg4d5h7d54s2		23s4fgsd564fds6	
Justificatif de méta-identité	Certificat numérique *uuu*.cnrs.fr		Certificat numérique *xxx*.cnrs.fr		« Je@nPerr1n »	

- **Single Sign-On (SSO)**

L'approche Single Sign-On est similaire à une fédération d'identité, mais aucune correspondance d'identité n'est nécessaire, car il n'existe qu'un seul fournisseur d'identité. Dans cette architecture, un utilisateur n'a besoin de s'authentifier qu'une seule fois (en anglais « single sign-on ») auprès d'un fournisseur de service. Il est alors authentifié *de facto* auprès des autres fournisseurs de service.

Le modèle Single Sign-On peut être associé au modèle de fédération d'identité, permettant une authentification unique inter-domaine.

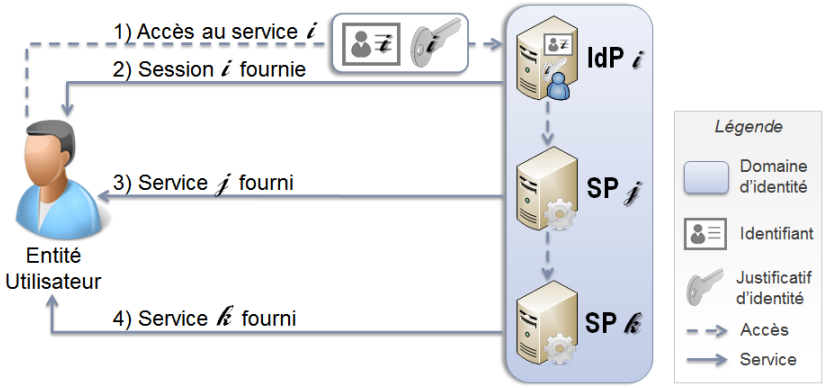

Figure 8 - Modèle de gestion d'identité : « Single Sign-On »

Dans le cadre de l'exemple décrit précédemment, ce modèle d'identité permet d'utiliser un unique couple identifiant-justificatif d'identité quel que soit le service demandé au sein du domaine d'identité. Ainsi, comme dans le cas d'une fédération, l'organisation peut déployer un domaine de SSO « Ingénieur » pour l'ensemble des services liés aux activités d'ingénieur. Dans ce cas, la personne ne manipule qu'un seul couple identifiant-justificatif d'identité (« jean.perrin@*uuu*.cnrs.fr » - Certificat numérique « *uuu*.cnrs.fr ») lors de la connexion au service « Crac ». L'identité correspondante (« Ingénieur ») est alors automatiquement reconnue par le service « Doc », permettant de l'utiliser sans phase d'authentification préalable.

Tableau VII - Synthèse de l'exemple pour le modèle de Single Sign-On

Fournisseur de service	Crac	Doc	Bdg	Ddm	Ret	Cge
Domaine d'identité	Ingénieur		Manager		RH	

Fournisseur de service	Crac Doc	Bdg Ddm	Ret Cge
Fournisseur d'identité	IdP Chercheur	IdP DU	IdP RH
Nom	PERRIN	PERRIN	PERRIN
Prénom	Jean-Baptiste	J.B.	Jean-Baptiste
Affectation	Département *uuu*	Département *xxx*	-
Identifiant fourni	jean.perrin@*uuu*.cnrs.fr	j-b.perrin@*xxx*.cnrs.fr	153545
Justificatif d'identité fourni	Certificat numérique *uuu*.cnrs.fr	Certificat numérique *xxx*.cnrs.fr	« Je@nPerr1n »

2.3 Cadre réglementaire

La loi française Informatique et Libertés n° 78-17 du 6 janvier 1978 modifiée par la loi du 6 août 2004 définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Cette loi est applicable dès qu'il existe un traitement automatisé ou un fichier manuel, c'est-à-dire un fichier informatique ou un fichier « papier » contenant des informations personnelles relatives à des personnes physiques.

La Commission Nationale Informatique et Libertés (CNIL) veille à la mise en œuvre des principes de la loi Informatique et Libertés dont ceux :

- de pertinence des données : « les données personnelles doivent être adéquates, pertinentes et non excessives au regard des objectifs poursuivis »,
- de durée limitée de conservation de données : « les informations ne peuvent pas être conservées de façon indéfinie dans les fichiers informatiques ; une durée de conservation doit être établie en fonction de la finalité de chaque fichier » (par exemple : le temps de la présence du salarié pour une application de gestion des carrières, cinq ans pour un fichier de paie, deux ans après le dernier contact avec le candidat à un emploi pour un fichier de recrutement),
- de sécurité et de confidentialité : « l'employeur, en tant que responsable du traitement, est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisés ». L'article 34 précise que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».
- du principe de transparence : la loi garantit aux personnes l'accès à l'information relative aux traitements auxquels sont soumises des données les concernant et les assure de la possibilité d'un contrôle personnel. Le responsable de traitement des données personnelles doit avertir ces personnes dès la collecte des données et en cas de transmission de ces données à des tiers.

L'article 226-17 du code pénal réprime la non observation de ces principes de précaution par des dispositions particulièrement lourdes. En effet, « le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ». Par ailleurs, l'article 226-22 est également applicable, suite à la plainte d'une victime d'indiscrétion, même s'il s'agit d'une

simple négligence. Il précise que « le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Le Correspondant Informatique et Libertés (CIL) se positionne en intermédiaire entre le responsable des traitements des données concernées et la CNIL. Il doit avoir une connaissance approfondie de l'organisation responsable des traitements. De ce fait, il doit être un employé. Il est responsable de la création et de la mise à jour de la liste des traitements effectués, ainsi que de la publication de cette liste. Il veille également au respect des principes de la protection des données personnelles. Il a un rôle d'information pour les personnes au sujet de l'existence de leurs droits d'accès, de rectification et d'opposition.

3. Gestion des accès

3.1 Définitions

3.1.1 Ressources et gestion des accès

Afin de permettre de réaliser ses projets en toute sécurité, une organisation doit gérer les accès aux ressources dont elle dispose.
Comme évoqué précédemment lors de la définition du concept d'identité, une ressource désigne un fournisseur de service identifié par un libellé tel qu'un système d'information ou de communication.
La gestion des accès permet de s'assurer de mettre à disposition de chacune des personnes impliquées dans les projets de l'organisation, à tout instant, tous les moyens nécessaires à la réalisation de la mission qui leur a été confiée, et que ces moyens soient à chaque instant limités au juste nécessaire [5].

Par la politique de gestion des accès, les accès aux ressources sont limités par des contraintes établies par l'organisation dont les définitions sont développées dans les paragraphes suivants :

- Mode d'authentification et contrôle d'accès ;
- Périmètre d'accès ;
- Rôles, profils et groupes autorisés.

3.1.2 Comptes utilisateurs

Un compte est un ensemble d'informations composé d'« un identifiant, un mot de passe (ou un justificatif d'identité d'une autre nature) et plusieurs attributs supplémentaires en fonction de l'environnement dans lequel il est créé » [6]. Un compte peut donc être la représentation informatique d'une identité. Il existe trois principaux types de comptes : le compte utilisateur, le compte d'administration et le compte de service.
Le compte utilisateur est associé à une entité utilisateur. Il est utilisé pour se connecter aux ressources d'un contexte auprès desquelles la personne est habilitée.
Le compte global est un compte utilisateur unique qu'une personne utilise pour tous les processus d'authentification et autorisation de l'ensemble des ressources de l'organisation.
Le compte d'administration permet à une entité d'accéder à une unique ressource et d'en assurer la gestion. Cependant, il n'est pas associé à une entité, ce qui implique qu'il ne doit pas être connu des référentiels d'identité. Son utilisation doit être limitée aux tâches techniques qui ne peuvent pas être réalisées au travers des rôles (cf. définition ci-après) d'administration. Il est souvent créé lors de l'installation d'une application avec des valeurs d'attributs prédéfinies. C'est pour cette raison qu'il est préférable de désactiver tous les comptes de cette nature. En effet, les mots de passe étant affectés avec une valeur par défaut à l'installation, ils sont connus de tous et présentent donc une faille de sécurité importante [7].
Le compte de service fonctionnel ou technique est associé à une entité ressource. Il permet de s'authentifier (ou simplement s'identifier) auprès d'une autre ressource pour accéder à ses services. Les droits d'accès octroyés à ce compte sont limités. Aucune personne n'est autorisée à utiliser ce type de compte.

[7] G. Harry. *Failles de sécurité des applications Web*. CNRS, 38 pages, 2012

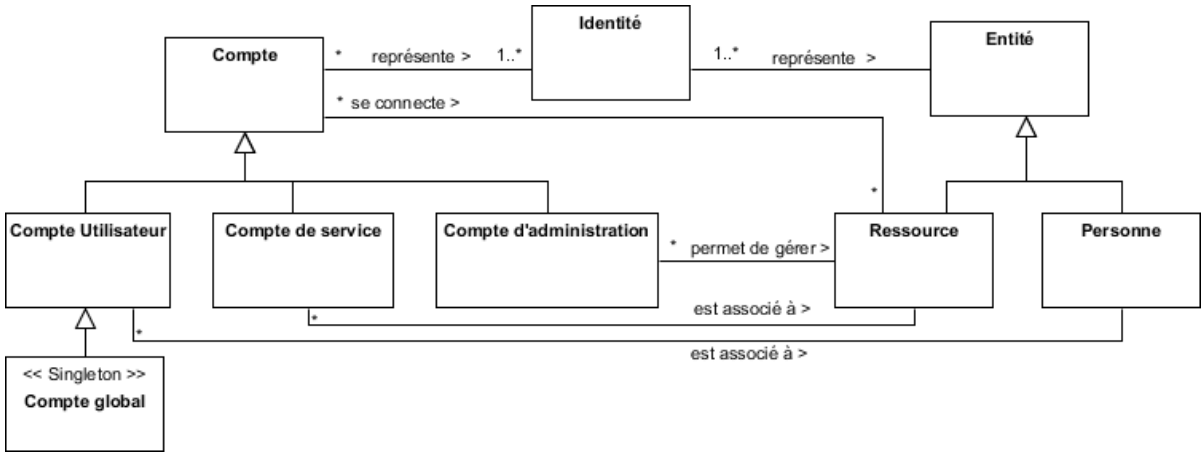

Figure 9 - Diagramme de classe des comptes

3.1.3 Habilitations et contrôle d'accès

Le CLUSIF [6] décrit une habilitation comme un droit d'effectuer une action sur une ressource. Elle est associée à un périmètre qui limite quand et comment cette ressource peut être utilisée par une entité. Les habilitations sont attribuées en fonction des besoins des métiers au sein de l'organisation.

F. Ferraiolo, D. R. Kuhn et R. Chandramouli [8] définissent un contrôle d'accès comme un processus pour vérifier les habilitations affectées à une entité.

Les contrôles d'accès sont un des moyens d'assurer la sécurité de l'information qui peut être définie par trois concepts complémentaires :

- La confidentialité est l'assurance qu'une information ne peut être lue que par les entités qui en ont le droit ;
- L'intégrité est la protection de l'information contre des modifications par des entités qui n'en ont pas le droit ;
- La disponibilité est la capacité à mettre l'information à disposition quand les entités en ont besoin.

Les contrôles d'accès permettent d'assurer la confidentialité et l'intégrité de l'information. La disponibilité de l'information dépend de celle des mécanismes mis en œuvre pour assurer les contrôles d'accès. En effet, si le moyen de réaliser les contrôles d'accès est inutilisable, alors l'information ne peut être ni lue, ni modifiée, la rendant indisponible.

3.1.4 Rôle, profil, groupe et périmètre

Les termes de rôle, de profil et de groupe sont souvent confondus, alors que ce sont des concepts manipulés régulièrement dans la gestion des identités et des accès.

Un rôle est un ensemble d'habilitations nécessaires à un type d'utilisation d'une ressource. Un rôle applicatif est un rôle propre à une seule fonction et appartient à une seule application. Il est recommandé d'utiliser les rôles applicatifs comme unique moyen d'accorder des habilitations à un compte. De ce fait, les rôles permettent de maîtriser les permissions octroyées et de déceler les conflits entre les droits.

De même, un rôle ne doit pas être octroyé directement à un compte utilisateur. Il est préférable de les attribuer au travers des profils métiers qui regroupent l'ensemble des rôles

[8] D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli. *Role-Based Access Control, Second Edition*. Artech House, 381 pages, 2007

nécessaires à la réalisation d'une mission. Un profil correspond donc généralement à une fonction exercée au sein d'une organisation.

Lorsque des entités doivent obtenir les mêmes habilitations spécifiques, mais que leurs profils ne correspondent pas, elles peuvent être regroupées en groupes statiques ou dynamiques. Par exemple, des personnes participant à un projet ont besoin de pouvoir partager des documents au sein d'un espace de travail collaboratif. Un groupe statique est constitué par une liste exhaustive des comptes utilisateurs devant obtenir une habilitation particulière. L'utilisation de ce type de groupe n'est pas recommandée lorsque la liste doit évoluer souvent. Dans ce cas, il est préférable d'opter pour un groupe dynamique qui est généré sur la base d'un critère tel que la présence ou la valeur d'un attribut dans les comptes utilisateurs. Dans le cadre de l'exemple sur les projets, tous comptes utilisateurs possédant l'attribut « Administrateur Système et Réseau » font partie du groupe du même nom qui leur donne le droit de déposer et de modifier des documents dans le répertoire « Architecture informatique » et leur permet également de lire tous les comptes-rendus d'avancement du projet. Par contre, une liste statique de comptes utilisateur établie quels sont ceux qui ont la capacité de déposer et modifier ces rapports. Les groupes permettent donc de faciliter la gestion massive d'habilitations indépendamment des rôles.

Comme évoqué précédemment, une habilitation est soumise à un périmètre applicatif qui restreint les capacités d'utilisation d'une ressource.
Le périmètre temporel interdit les accès à une ressource en dehors des périodes autorisées. Il peut être assigné à un compte utilisateur, un rôle ou une ressource. Les restrictions sont exprimées en fonction de trois critères cumulables :

- La période, définie par une date de début et une date de fin, n'autorise l'utilisation de la ressource cible que si la tentative d'accès est opérée entre ces deux dates ;
- La plage horaire, définie par une heure de début et une heure de fin, n'autorise l'utilisation de la ressource cible que si la tentative d'accès est réalisée entre les heures spécifiées ;
- Le calendrier, défini par une liste de jours calendaires, une liste de semaines ou une liste de mois, n'autorise l'utilisation de la ressource cible que si la tentative d'accès est opérée un jour appartenant à une des listes citées.

Le périmètre géographique limite les accès à une ressource en fonction du lieu à partir duquel un utilisateur tente de se connecter. Il peut être affecté à un compte ou un rôle. L'ensemble des habilitations liées au profil du compte utilisateur évolue alors en fonction du lieu de présence de la personne auquel il appartient, permettant ainsi par exemple d'empêcher la manipulation d'informations confidentielles à partir de points d'accès non fiables. Les restrictions sont de trois types :

- Le poste de travail physique, identifié par un numéro d'inventaire ou une adresse IP, à partir duquel l'organisation souhaite autoriser ou interdire certaines opérations ;
- Un lieu, un groupe de lieu ou une zone géographique dans laquelle le poste de travail doit se situer lors de la tentative de connexion pour obtenir le droit d'utiliser la ressource cible ;
- Une typologie d'accès pour permettre les accès à la ressource. Il peut s'agir d'un accès par le réseau de l'organisation, un réseau mis à disposition par un partenaire ou un réseau privé dédié.

Le périmètre fonctionnel limite l'exécution de traitements applicatifs en fonction de la valeur ou de la nature des informations fournies en paramètre. Il peut être assigné à un rôle. Les données peuvent être relatives par exemple à un secteur géographique, à l'affectation au sein de l'organisation ou au type d'appareil utilisé pour se connecter.

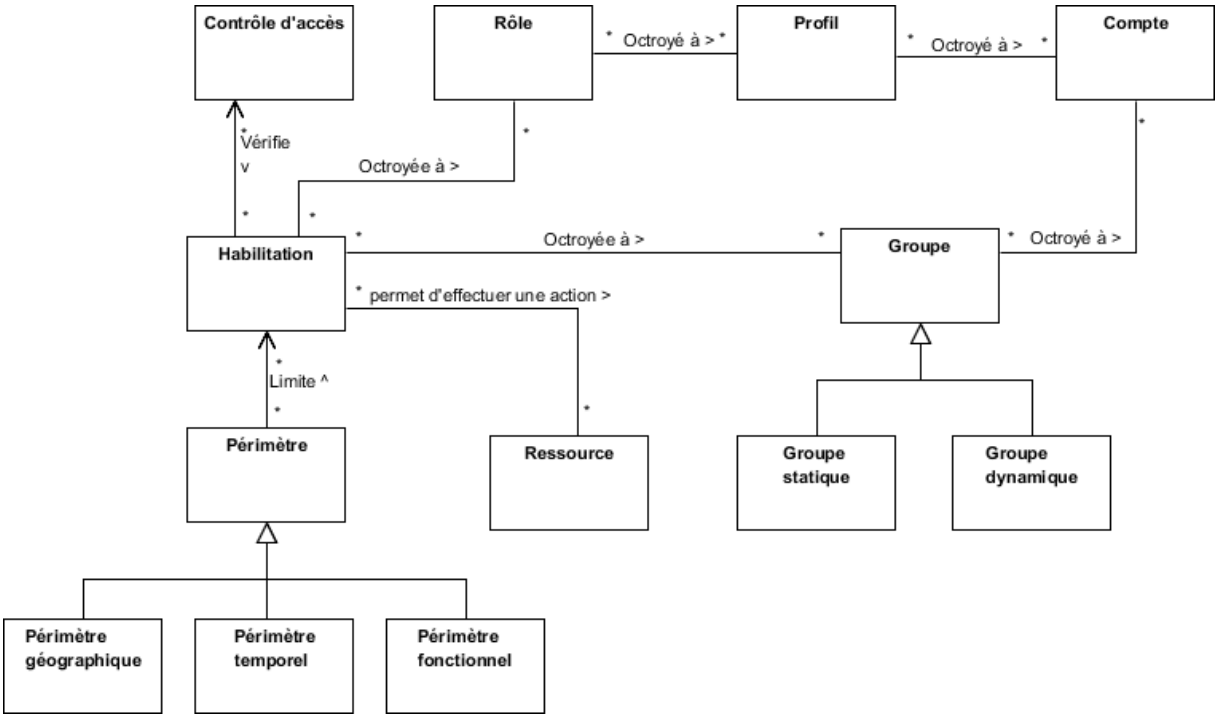

Figure 10 - Diagramme de classe des habilitations

3.1.5 Authentification et autorisation

Comme évoqué lors de la définition de la gestion d'identité, l'authentification est le processus qui permet de vérifier que l'identité revendiquée par une entité est légitime. Elle est basée sur un ou plusieurs mécanismes de reconnaissance :

- Quelque chose que l'entité connaît comme par exemple un mot de passe ou un numéro personnel d'identification (code PIN) ;
- Quelque chose que l'entité possède, telle qu'une carte ou une clé ;
- Une caractéristique physique telle qu'une empreinte digitale ou rétinienne.

L'authentification est plus sûre si plusieurs techniques sont utilisées conjointement [6]. En effet, un mot de passe peut être deviné, une clé peut être perdue et une reconnaissance faciale peut être faussée à cause des marges d'erreur. Aussi, l'utilisation d'une technique ne fournit pas un niveau de sécurité suffisant. Il faut en utiliser plusieurs pour diminuer les risques d'erreur ou de falsification. Le mode d'authentification peut être déterminé en fonction du rôle associé aux comptes utilisateurs ou de la ressource utilisée.

L'autorisation est le processus responsable d'établir les habilitations dont dispose une identité au travers d'un compte et du profil qui lui est associé ou des groupes auxquels il appartient. Ce processus détermine donc ce qu'une identité a le droit de faire pour chacune des ressources qui lui est mise à disposition. Des modèles d'autorisation d'accès sont exposés dans le paragraphe « Modèles des gestions d'accès ».

Ces deux concepts sont utilisés conjointement pour les contrôles d'accès, le processus d'autorisation étant dépendant du bon fonctionnement de l'authentification. En effet, si le moyen d'authentifier une identité n'est pas sûr, alors il n'est pas possible de garantir que les autorisations soient accordées à la bonne entité. Dans ce cas, le contrôle d'accès ne permet pas d'assurer la confidentialité et l'intégrité des informations qu'il doit protéger.

3.1.6 Exemples

Pour la gestion, l'organisation met à disposition plusieurs ressources : un service de gestion du budget du département nommé « Bdg » et un service de rapports décisionnels pour le pilotage de l'organisme nommé « Rpt ». Le service « Bdg » offre la possibilité de saisir des commandes et de produire des rapports analytiques détaillés ou synthétiques sur les dépenses et les subventions. Pour se connecter à ce service, il est nécessaire de disposer d'un compte. Ainsi, pour un responsable de département connu sous l'identité « Manager du département *xxx - J.B. Perrin* » un compte utilisateur « Bdg-JBP » est créé. Pour son assistante, l'organisation produit l'identité « Gestionnaire du département *xxx - G. Mineur* » à laquelle est lié le compte utilisateur « Bdg-GM ». Par ailleurs, l'entreprise dispose d'une équipe de la production applicative responsable du maintien en condition opérationnelle (MCO) des ressources à laquelle appartient l'« Exploitant Joseph Licklider ». A ce titre, l'équipe dispose d'un compte d'administration « Bdg-ADMIN ». De plus, pour produire des rapports au niveau de l'établissement, la ressource « Rpt » doit accéder à la ressource « Bdg », ce qui est réalisable au travers du compte de service « Bdg-READ ».

Tableau VIII - Exemple de comptes utilisateurs

Compte Information	Bdg-GM	Bdg-JBP	Bdg-READ	Bdg-ADMIN
Identité représentée	Gestionnaire du département *xxx* *G. Mineur*	Manager du département *xxx* *J.B. Perrin*	Ressource « Rpt »	*Non applicable*
Nom	G. Mineur	J.B. Perrin	Rapport	ADMIN
Affectation	Département *xxx*	Département *xxx*	-	Production applicative
Type de compte	Utilisateur	Utilisateur	Service	Administration
Personne manipulant le compte	Gabrielle MINEUR	Jean-Baptiste PERRIN	*Non applicable*	Joseph LICKLIDER
Ressource cible	Service « Bdg »	Service « Bdg »	Service « Bdg »	Service « Bdg »
Identifiant	GM	JBP	READ	ADMIN
Justificatif d'identité	« G@brie11e »	« @zer1yuioP »	« f&jdsu_oehyè »	« myEXP1@cnt »

Le service « Bdg » offre la possibilité de :

- lire (action « read ») ou saisir/modifier (action « write ») des commandes pour un périmètre fonctionnel limité au département et à l'année,
- lire (action « read ») ou saisir/modifier (action « write ») les crédits alloués pour un périmètre fonctionnel limité au département et à l'année,
- lire (action « read ») ou générer (action « execute ») des rapports sur le budget pour un périmètre fonctionnel limité au département,
- lire (action « read ») les informations techniques des journaux évènementiels,
- Démarrer et arrêter (action « execute ») le service « Bdg ».

Les habilitations liées à ces fonctionnalités sont octroyées au travers de rôles valides uniquement pour la ressource « Bdg ». Le tableau suivant montre l'affectation des habilitations et leur périmètre sur les rôles « Intendance Département », « Management Département », « Lecture budget Département », « Rapport budget Département » et « MCO ».

Tableau IX - Exemple de rôles applicatifs

Profil / Rôle	Intendance département	Manager département	Lecture budget département	Rapport budget département	MCO
Périmètre	Département	Département	Département	Département	-
Commandes	read, write	-	read	-	-
Crédits	-	read,write	read	-	-
Rapport	-	-	read	execute	-
Informations techniques	-	-	-	-	read
Service	-	-	-	-	execute

Un compte utilisateur ayant le profil « Manager », tel que « Bdg-JBP », doit obtenir les habilitations à saisir les crédits alloués à son département, à lire tout type d'information liées à son département durant son mandat et à en générer les rapports. Pour ce faire, ce profil se voit octroyer les rôles « Management département », « Lecture budget département » et « Rapport budget département ». Conjointement, un compte utilisateur ayant le profil « Gestionnaire », tel que « Bdg-GM », doit obtenir l'habilitation à saisir des commandes et à visualiser des rapports sur le budget du département d'affection et l'année en cours. A cet effet, ce profil dispose des rôles « Intendance département » et « Lecture budget département ». Un compte ayant le profil « Lecture », tel que le compte de service « Bdg-READ », doit disposer des habilitations permettant de lire des informations budgétaires pour l'ensemble des départements dans l'application « Bdg ». Pour répondre à ce besoin, ce profil dispose du rôle « Lecture budget département » sur l'ensemble des départements enregistrés. Un compte d'administration, utilisé notamment par l'« Exploitant Joseph Licklider », doit être habilité à démarrer et arrêter le service « Bdg », à accéder aux informations techniques liées aux évènements applicatifs et à pouvoir lancer la génération de rapports en cas de défaillance. Ainsi, le profil « Production applicative » possède les rôles « MCO » et « Rapport budget département ».

Tableau X - Exemple de profils

Profil / Rôle	Gestionnaire	Manager	Lecture	Production applicative
Intendance département	Périmètres dept, année	-	-	-
Management département	-	Périmètres dept, année	-	-
Lecture budget département	Périmètres dept, année	Périmètres dept, année	Sans limite	-
Rapport budget département	-	Périmètres dept, année	-	Périmètres dept, année
MCO	-	-	-	Sans limite

3.2 Modèles

Comme évoqué précédemment, le contrôle des accès revêt plusieurs aspects pour assurer la sécurité des ressources et des informations. Il repose sur l'utilisation de différentes notions telles que les identités avec les modèles IBAC, les rôles avec le modèle RBAC ou les périmètres avec des modèles tels qu'ABAC ou OrBAC.

3.2.1 Identity based access control (IBAC)

F. Cuppens et N. Cuppens-Boulahia [9] présentent le modèle IBAC comme étant historiquement le premier type de contrôle d'accès. Bien qu'introduit par B. Lampson en 1971, il est toujours utilisé par les systèmes d'exploitation sur les marchés des ordinateurs personnels, avec Microsoft Windows par exemple, et des serveurs avec les systèmes Unix et Linux. Ce modèle repose sur une matrice composée d'un ensemble fini d'entités, de ressources cibles et de règles. Il conduit à l'établissement d'une liste exhaustive d'autorisations d'accès (ACL : « Access Control List » en anglais). Cela implique que tout accès non explicitement autorisé est interdit. Ainsi, les habilitations sont affectées directement aux comptes utilisateurs. Ainsi chaque droit est assigné nominativement.

Le tableau suivant est un exemple de matrice ACL pour les comptes utilisateurs et habilitations décrits dans l'exemple décrit précédemment. Ainsi le responsable du département *xxx* nouvellement nommé ne pourra saisir les crédits que pour l'année en cours mais pourra consulter les crédits et rapports de l'ensemble des années.

Tableau XI - Exemple de matrice ACL du modèle IBAC

	Bdg-GM	Bdg- JBP	Bdg-READ	Bdg-ADMIN
Commandes département *xxx* 2011	read, write	read	read	-
Commandes département *xxx* 2012	read, write	read	read	-
Crédits département *xxx* 2011	read	read	read	-
Crédits département *xxx* 2012	read	read, write	read	-
Rapport département *xxx* 2011	read	read	-	execute
Rapport département *xxx* 2012	read	read,execute	-	execute
Informations techniques	-	-	-	read
Service	-	-	-	read

Une des implémentations du modèle IBAC est le contrôle d'accès discrétionnaire (DAC : « Discretionary Access Control » en anglais) qui repose sur la notion de propriétaire de la ressource. Ce dernier a le contrôle total sur la ressource qu'il a créée et dont il est responsable. Il détermine ainsi quelle entité a droit à quel type d'action sur sa ressource.

La complexité des ACLs augmente en fonction du nombre d'identités et du nombre de ressources puisqu'il faut lister exhaustivement les autorisations pour chacune des combinaisons. En effet, lors la mise à disposition d'une nouvelle ressource ou à l'arrivée d'un nouvel utilisateur, la liste des autorisations doit être mise à jour. Les modèles qui suivent permettent de faciliter la gestion des habilitations.

3.2.2 Mandatory Access Control (MAC)

Dans le cas où le propriétaire d'un système d'information ne doit pas être responsable de la gestion de la sécurité sous-jacente, les modèles de type MAC permettent de limiter les accès en fonction de la sensibilité des données. Dans cet objectif, les entités cibles sont hiérarchisées en différents niveaux de sécurité (MLS : « multi-level security » en anglais) appelés labels.
En 1973, D. Bell et L. LaPadula ont développé un modèle où un niveau minimum de sécurité est requis pour avoir le droit d'accéder à la ressource. Ce niveau définit le niveau d'habilitation de l'utilisateur. De même, un niveau de sécurité est affecté à la ressource. Ce

[9] F. Cuppens, N. Cuppens-Boulahia. Les modèles de sécurité. Dans *Sécurité des systèmes d'information, (Traité IC2, série Réseaux et télécoms)*. Hermès, pages 13-48, 2006

niveau détermine le niveau de classification de la ressource. L'utilisateur n'a alors accès à la ressource que si son niveau d'habilitation est supérieur ou égal au niveau de classification de la ressource. De plus, pour une application, un niveau d'exécution, appelé niveau courant, est également défini. Le niveau courant d'une application est toujours inférieur ou égal au niveau d'habilitation de l'utilisateur responsable de l'exécution de l'application. La condition « no read up » implique qu'une application ne peut accéder en lecture à des informations que si le niveau courant de l'application est supérieur ou égal au niveau de classification de la ressource qui gère ces données. De même, la condition « no write down » suppose qu'une application ne peut transmettre des informations à une ressource que si son niveau courant est inférieur ou égal au niveau de classification de la ressource cible. Ce modèle de contrôle des accès est également appelé Rule Based Access Control (RuBAC), car les accès sont régis par des règles.

Dans le cadre des restrictions évoquées dans l'exemple de comptes utilisateurs décrit précédemment, les niveaux d'habilitation peuvent être définis sur cinq niveaux. Ainsi, les informations gérées par la ressource « Bdg » sont classifiées de niveau 3. Les comptes utilisateurs devant s'y connecter doivent donc disposer d'une habilitation de niveau supérieur ou égal à 3. Ainsi, le compte « Bdg-GM » dispose du niveau d'habilitation 4, « Bdg-JBP » du niveau d'habilitation 5. Le compte « Bdg-ADMIN » responsable de l'exécution du service a un niveau d'habilitation minimum, ce qui implique qu'il a le niveau d'habilitation 3. Le niveau courant de l'application « Bdg » doit donc être inférieur ou égal au niveau d'habilitation 3 du compte « Bdg-ADMIN ». Pour respecter la contrainte « no read up », le niveau courant de l'application « Bdg » doit également être supérieur au niveau de classification 3 des informations, ce qui implique que le niveau courant de l'application doit être fixé à 3. Par ailleurs, la contrainte « no write down » implique que la ressource « Rpt », qui doit être en mesure lire des données de la ressource « Bdg », doit avoir un niveau de classification supérieur ou égal au niveau courant 3 de l'application « Bdg ». De plus, étant établi que l'accès aux informations de la ressource « Rpt » requiert le niveau d'habilitation le plus élevé, le niveau de classification de la ressource « Rpt » est imposé à 5 obligeant à définir le niveau courant de l'application « Rpt » à 5.

Tableau XII - Exemple d'implémentation du modèle MAC

Niveau	Compte « Bdg-GM »	Compte « Bdg-JBP »	Compte « Bdg-ADMIN »	Ressource « Bdg »	Ressource « Rpt »
Habilitation	4	5	3		
Classification				3	5
Courant				3	5

En 1986, D. Bell propose une version étendue de ce modèle où le niveau courant d'une application n'est plus déterminé par un unique niveau mais par un intervalle de niveaux, ce qui offre plus de flexibilité. Dans ce cas, une application peut accéder en lecture à toute information dont la classification est comprise entre la borne inférieure et la borne supérieure du niveau courant de l'application. Ce modèle est proche de celui utilisé actuellement par le système de gestion de bases de données Oracle via l'option Label Security pour segmenter les données.

3.2.3 Role Based Access Control (RBAC)

Contrairement au modèle IBAC où les habilitations sont octroyées directement à l'utilisateur, dans le modèle RBAC, élaboré par le National Institute of Standards and Technology (NIST) à partir de 1992 [7], les habilitations sont affectées à des rôles. La gestion

des habilitations est alors simplifiée. En effet, par exemple, lors de l'enregistrement d'un nouvel utilisateur, il suffit de lui attribuer les rôles nécessaires à la réalisation de sa mission au lieu de lui octroyer l'ensemble des habilitations sous-jacentes. Ainsi, dans l'exemple des rôles applicatifs, lors de sa prise de fonction, un gestionnaire se voit attribuer le rôle « Intendance département » au travers de son compte utilisateur. Il a alors accès en lecture, en saisie aux commandes effectuées par le département pour l'année en cours.

Par ailleurs, le NIST propose plusieurs déclinaisons du modèle RBAC [10]. Le modèle RBAC hiérarchique (HRBAC : « hierarchical role based access control » en anglais) prend en compte les liens de parenté entre rôles. Ainsi lorsqu'une habilitation est octroyée ou enlevée à un rôle parent, les rôles fils en héritent et acquièrent, ou respectivement perdent, cette habilitation. HRBAC supporte deux types de hiérarchie. La variante générale (« General Hierarchical RBAC » en anglais) accepte des héritages ascendants et descendants multiples. Par opposition, dans la variante limitée (« Limited Hierarchical RBAC » en anglais) un rôle ne peut hériter que d'un seul parent. Dans le cadre de l'exemple des rôles applicatifs, le rôle « Lecture budget département » est commun aux profils « Gestionnaire » et « Manager ». Ce rôle est donc nécessaire lorsque les rôles « Intendance département » et « Management département » sont affectés. La modélisation de ces rôles peut alors être simplifiée en définissant « Lecture budget département » comme rôle parent de « Intendance département » et « Management département ». Seuls ces deux derniers rôles sont alors octroyés, car ils héritent des habilitations du rôle parent « Lecture budget département ».
La seconde déclinaison du modèle RBAC permet la gestion des conflits d'intérêts induits par des rôles incompatibles octroyés à un même utilisateur. En effet, le modèle RBAC avec contraintes (CRBAC : « constrained role based access control » en anglais) assure la séparation des responsabilités (SoD : « Segregation of Duty » en anglais) en empêchant le cumul d'habilitations contradictoires. Ainsi, dans les exemples de rôle décrits précédemment, un compte ne peut pas être associé en même temps aux rôles « Intendance département » et « Management département » qui représentent deux fonctions dans l'organisme qui ne peuvent être exercées par une seule personne au sein d'un département. Par ailleurs, la mise en œuvre de la séparation statique des responsabilités (en anglais : « static separation of duty ») implique la définition de règles d'affectation de rôles. L'administrateur responsable des accès ne peut alors pas affecter des rôles incompatibles. Ainsi un utilisateur appartenant à un rôle ne peut pas se voir attribué un rôle rendu interdit par ces règles. La séparation dynamique des responsabilités (en anglais : « dynamic separation of duty ») permet de ne pas retirer un rôle en cas de non-respect des règles, mais simplement de le révoquer temporairement au moment où l'utilisateur demande à se connecter à la ressource.

La mise en place d'un système de contrôle d'accès basé sur le modèle RBAC au sein d'une organisation requiert la mise en œuvre d'une stratégie de définition des rôles (en anglais : « role engineering ») qui n'est pas une tâche aisée. Il existe deux principaux types d'approche « bottom-up » (du bas vers le haut) et « top-down » (du haut vers le bas) complétés par des approches hybrides.
Pour les organisations disposant déjà d'un système de gestion des droits d'accès la démarche bottom-up permet de construire des rôles en examinant les habilitations existantes. Des outils de rolemining permettent d'accélérer cette recherche [11]. Ils exploitent des algorithmes de datamining, chacun ayant un objectif différent, tel que minimiser le nombre de rôles

[10] D. F. Ferraiolo , R. Sandhu , S. Gavrila , D. R. Kuhn , R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security* v.4 n.3, pages 224-274, 2001

[11] M. Frank, J. M. Buhmann , D. Basin. On the definition of role mining. *Proceeding of the 15th ACM symposium on Access control models and technologies*, pages 35-44, 2010

découverts, établir les hiérarchies de rôles ou découvrir un nombre faible de rôles possédant le plus grand dénominateur commun d'habilitations. Cependant les droits inutilisés résiduels peuvent perturber cette analyse et mener à des définitions de rôles qui n'ont aucune correspondance avec des concepts métier.
A l'inverse, la démarche top-down étudie par itérations successives les fonctions métiers pour en déduire les habilitations et les rôles inhérents. La difficulté réside alors dans l'exhaustivité et la granularité des rôles. En effet, des rôles trop larges admettent trop de droits et des rôles trop restreints vont augmenter la difficulté d'administration.
L'approche hybride consiste à rechercher les rôles par l'approche bottom-up et les affiner ensuite par confrontation avec les informations collectées par l'approche top-down.

Le modèle RBAC est aujourd'hui un standard qui permet notamment la mise en conformité vis-à-vis de la loi Sarbanes-Oxley (cf. paragraphe « cadre réglementaire »). Il s'adresse plus particulièrement aux organisations dont la définition des métiers et des missions est figée et évolue peu. Dans le cas contraire, des exceptions seront nécessaires pour autoriser des accès spécifiques ou temporaires. Cette situation implique la mise en place d'une liste annexe de contrôle d'accès, comme dans le modèle IBAC. Il n'est alors plus possible de se baser sur les définitions des rôles et des profils pour déterminer qui possède quel type d'accès sur quelle ressource.

3.2.4 Attribute Based Access Control (ABAC)

Le modèle ABAC, défini par L. Wang, D. Wijesekera, S. Jajodia [12], propose de définir les droits d'accès en fonction des caractéristiques des identités. A l'instar du modèle IBAC, la politique des droits d'accès peut être matérialisée par une matrice, mais en ne se basant pas sur les identités. De ce fait, les droits d'accès à une ressource ou un service sont définis pour un ou plusieurs attributs que les identités sont susceptibles de posséder. Ce paradigme offre donc plus de flexibilité. De plus, en définissant un attribut se rapprochant de la notion de rôle, ABAC permet de simuler le comportement d'un modèle RBAC, mais le généralise en ne limitant pas les droits d'accès aux seuls utilisateurs présents dans l'organisation. Il permet notamment de déterminer des droits d'accès avec une granularité plus fine. De plus, en définissant un rôle comme un ensemble d'attributs, il est plus facile de gérer les conflits. Par ailleurs, la gestion des droits d'accès est facilitée, car elle ne nécessite pas d'informations supplémentaires. Cependant, la sécurité des accès repose alors sur les valeurs affectées aux attributs et donc sur la qualité et l'intégrité des informations liées aux identités.

Dans le cadre des exemples décrits précédemment, le modèle ABAC implique que l'octroi de l'attribut « Resp dept » à un compte utilisateur a pour effet de donner accès automatiquement aux lignes de crédits et rapports. L'attribut « Resp dept » peut être perçu comme la matérialisation du profil « Manager ».

3.2.5 Organization Based Access Control (OrBAC)

Avec le modèle OrBAC [9], l'organisation est perçue d'un point de vue abstrait comme un ensemble d'activités que les rôles ont la permission, interdiction ou obligation de réaliser au travers des vues. Tout comme dans RBAC, il est possible d'utiliser la notion d'héritage pour les rôles. Concrètement, les habilitations sont octroyées à des sujets pour des actions sur des objets au travers de matrices à trois dimensions.

---

[12] L. Wang, D. Wijesekera, S. Jajodia. A logic-based framework for attribute based access control. *Proceedings of the 2004 ACM workshop on Formal methods in security engineering*, pages 45-55, 2004

Ce modèle semble permettre une gestion plus fine des droits d'accès, mais reste cependant peu implémentée.

3.2.6 Comparaison

Quelque soit le modèle implémenté au sein d'une organisation, l'objectif est de limiter la capacité d'action des entités utilisatrices des ressources au strict nécessaire pour réaliser leurs missions.
Dans le modèle IBAC, les contrôles d'accès reposent sur une liste exhaustive d'habilitations pour chaque compte autorisé.
Le modèle RBAC permet de diminuer la taille de liste des habilitations. Les contrôles d'accès sont réalisés sur les rôles attribués aux comptes. Les rôles applicatifs sont octroyés en fonction du profil métier.
Dans le modèle ABAC, les contrôles d'accès vérifient la présence et la valeur d'attributs applicatifs définis au niveau des comptes. Il est alors possible de simuler le comportement RBAC en calquant les attributs sur la définition des rôles.
Dans le modèle OrBAC les autorisations ou interdictions reposent sur des expressions contextuelles définies d'après la structure organisationnelle de l'établissement.
Le modèle MAC s'appuie sur le contrôle des flux. Des contraintes sont définies sur les données et les ressources. Le niveau d'habilitation d'un compte détermine alors s'il a le droit ou non d'accéder aux informations.

3.3 Cadre réglementaire

Bien que toutes les organisations ne soient pas concernées par les lois encadrant le comportement des entreprises privées, celles qui sont liées à la sécurité de l'information vont être exposées dans les paragraphes suivants afin de présenter les bénéfices et les contraintes liées à la gestion des accès. De plus, essayer de s'en rapprocher permet de diminuer les risques relatifs à la sécurité.

3.3.1 Loi américaine Sarbanes-Oxley

La loi Sarbanes-Oxley (SOx) fut votée par le congrès américain en juillet 2002 dans le but de redonner confiance aux investisseurs dans les marchés financiers suite aux scandales ENRON et WORLCOM. D. F. Ferraiolo, D. R. Kuhn et R. Chandramouli [8] précisent que la loi implique pour les entreprises cotées aux Etats-Unis et leurs filiales, y compris à l'étranger, ou qui empruntent sur le marché américain que les contrôles internes et les processus utilisés pour la production des rapports financiers soient certifiés auprès de la « Securities and Exchange Commission ». L'impact pour les systèmes d'information est un contrôle accru sur l'utilisation des logiciels dont l'organisation dépend pour ses données financières. Cela inclut également les outils de gestion des transactions, des données comptables, personnelles, d'inventaire et toute autre donnée qui peut être utilisée pour la production des rapports financiers. La surveillance doit assurer que tout changement soit opéré par une personne autorisée et selon un processus certifié.

Trois sections sont applicables aux systèmes d'information :

1. La section 302 implique que le comité exécutif certifie la complétude et l'exactitude des rapports financiers de l'organisation ;
2. La section 404 contraint l'organisation à maintenir « des procédures et des structures de contrôles internes adéquats pour la production de rapports financiers ». Les contrôles internes doivent être validés par des auditeurs externes pour assurer de leur authenticité, vérifier les renseignements sur site et avertir des insuffisances. Les responsables encourent des pénalités s'ils dissimulent l'absence ou l'insuffisance de contrôles ;

3. La section 409 requiert la présentation dans les plus brefs délais des rapports aux investisseurs et régulateurs de toute information concernant un changement dans les finances ou les opérations de l'organisation.

La section 404 de Sarbanes-Oxley est plus particulièrement liée à la gestion des identités et des accès. Dans ce paragraphe le terme « adéquat » concernant les contrôles internes n'est pas explicitement défini. Cependant, quelques bonnes pratiques sont citées dont les suivantes :

- Contrôles renforcés sur les identifiants et les permissions liées aux identifiants,
- Surveillance rigoureuse des attributions, mises à jour ou révocations de privilèges, incluant des capacités d'audit complet,
- Séparation des responsabilités pour l'accès ou la modification d'informations financières,
- Contrôle et audit des modifications présentant qui les a réalisées, quand et par quels moyens,
- Suivi et contrôle renforcé sur la mise à jour et les changements effectués sur les logiciels,
- Documentation sur la configuration et la maintenance des logiciels,
- Installation dès que possible des mises à jour de sécurité avec écriture dans les traces d'audit,
- Documentation complète sur les contrôles internes déficients qui réduisent les capacités de l'organisation à réaliser les objectifs cités précédemment.

La mise en œuvre de Sarbanes-Oxley peut être coûteuse, mais elle offre l'opportunité de mettre en place des processus internes sûrs. De plus, de part ces obligations, les organisations certifiées ISO-27001 (cf. paragraphe « Norme ISO-2700x ») respectent automatiquement Sarbanes-Oxley.

Les outils de gestion des identités et des accès des grands éditeurs sont compatibles avec la mise en conformité à Sarbanes-Oxley.

3.3.2 Accords internationaux Bâle II

Le comité Bâle sur le Contrôle Bancaire réunit les principales autorités de contrôle bancaire du monde. En 1988, il publia un premier accord, « Bâle I », sur la gestion des risques de crédit et la quantité de fonds propres minimaux pour les banques pour faire face à d'éventuelles pertes. En 1992, il fut décliné en différentes lois dans les pays du G10.

En 2004, le comité Bâle publia une seconde série d'accords, « Bâle II » qui prend en compte plus de catégories de risques et améliore le calcul et la gestion de ces risques [13]. Ils ont pour objectifs une meilleure transparence des entreprises, la protection des épargnants et un renforcement des contrôles. L'ensemble des obligations qui composent cette réforme est scindée selon trois piliers :

Pilier I : Disposer d'un montant de fonds propres pour couvrir les risques,
Pilier II : Les autorités disposent de pouvoirs renforcés pour imposer des exigences de fonds propres supérieurs à ceux envisagés par l'entreprise,
Pilier III : Obligation de publier des informations complètes sur la nature, le volume et les méthodes de gestion des risques ainsi que l'adéquation de leurs fonds propres.

Pour être conforme au premier pilier, l'organisation doit disposer d'une analyse économique des risques pour en connaître et ensuite limiter les impacts sur son bilan. Les risques sont répartis en trois catégories : risques de crédit, risques de marchés et risques

[13] G. Chamoret, F. Chavoutier, M. Copitet, J-P Godard, P. Grassart, J. Mauferon, L. Mourer, T. Ramard, G. Remy. *La réforme BÂLE 2, une présentation générale*. CLUSIF, 28 pages, 2004

opérationnels. Ces derniers incluent les risques relatifs à la sécurité des biens et des personnes, les risques informatiques liés aux développements et à la maintenance des programmes, traitements et services de télécommunications.
Chaque étape du processus de gestion des risques doit être prise en compte : l'identification, l'analyse, le traitement ainsi que son financement. Par ailleurs, les paragraphes 670 à 676 précisent que l'estimation des risques doit reposer, entres autres, sur des bases d'incidents et de pertes couplées à des outils d'analyse de scénario. Les bases d'incidents permettent de disposer d'un historique des sinistres constatés et leur fréquence, ce qui permet d'assurer un suivi des évolutions des différents risques et des mesures correctrices mises en œuvre. Les outils d'analyse de scénario doivent aider à construire des modèles statistiques de prévision des risques à partir de l'historique de la base des pertes.

L'obligation de transparence du troisième pilier implique de rendre compte dans un rapport des procédures de gestion des risques mises en place, notamment du système de contrôle interne. Ce dernier doit assurer un suivi des risques opérationnels, dont celui de conflit d'intérêt. Pour cela, l'organisation doit implémenter un système d'approbations et d'autorisations pour veiller à la séparation des responsabilités. L'organisation doit également protéger les accès et l'utilisation des actifs et des informations détenus par la banque.

En 2010, une première version du troisième accord, « Bâle III », fut publiée. Il ajuste les exigences de fonds, mais ne prend pas en compte les origines de la crise des « subprime ». Son impact est faible sur les systèmes d'information conformes à Bâle II.

3.3.3 Loi de sécurité financière (LSF)

La loi française n° 2003-706 du 1 août 2003 de sécurité financière s'applique à toutes les sociétés anonymes ainsi qu'aux sociétés faisant appel à l'épargne publique. Elle ne s'applique donc pas aux grands groupes. A l'instar de la loi américaine Sarbanes-Oxley, la loi de sécurité financière repose principalement sur une responsabilité accrue des dirigeants, un renforcement du contrôle interne et une réduction des sources de conflits d'intérêt.

Le contrôle interne doit permettre l'amélioration de la communication en temps réel et la fiabilisation de la production d'informations, répondant ainsi au besoin de transparence. Pour cela, l'organisation doit être capable de retracer le processus de génération de l'information depuis l'origine des données jusqu'aux décisions qui s'en sont suivies.

L'organisation doit donc mettre en place des outils de documentation permettant de décrire les activités et les processus inhérents de génération de rapports et de gestion de contenu pour conserver, gérer et mettre à disposition les informations de l'entreprise.

3.3.4 CRBF 97-02

Inspiré des démarches internationales comme celles du Comité de Bâle, le Règlement 97-02 du Comité de Réglementation Bancaire et Financière (CRBF) décrit les obligations de contrôle interne pour les établissements de crédit. Il est fondé sur cinq thèmes principaux : le système de contrôle des opérations et des procédures internes, l'organisation comptable et du traitement de l'information, les systèmes de mesure des risques et des résultats, les systèmes de surveillance et de maîtrise des risques ainsi que le rôle des organes exécutifs et délibérants.

Il en résulte qu'une entreprise assujettie doit mettre en œuvre un système de contrôle des opérations, des systèmes de surveillance et de maîtrise des risques ainsi qu'un système de documentation et d'information. De plus, l'organisme doit mettre en place des procédures de suivi des actions correctrices vis-à-vis des obligations de conformité.

Par ailleurs, l'article 4*n* stipule que l'établissement doit développer un plan de continuité de l'activité permettant la réalisation des tâches et services indispensables en cas de

scénario de crise, ainsi qu'un plan de retour planifié aux conditions normales quand le problème est résolu.

4. Bonnes pratiques

4.1 Normes

Bien qu'il ne soit pas nécessaire de suivre au sein d'une organisation les normes décrites ci-après, il est préférable de respecter le vocabulaire qui y est défini. De plus, il n'est pas forcément souhaitable d'atteindre le niveau d'exigence de la norme ISO-27002, notamment pour des raisons de coûts, mais tendre à s'en rapprocher permet de mettre en place un niveau de sécurité satisfaisant.

4.1.1 ISO-24760

La norme ISO-24760 citée précédemment est un ensemble de prescriptions concernant la gestion des identités divisé en trois parties.

La première partie (ISO-24760 A framework for identity management - Part 1 : Terminology and concepts [4], cf. annexe 1 « ISO-24760 ») est consacrée à la définition des concepts liés aux identités. Les notions décrites sont reprises et explicitées dans le présent document.

La seconde partie (ISO-24670 A framework for identity management - Part 2 : Reference architecture and requirements) ne sera publiée officiellement qu'en décembre 2013. Elle proposera une architecture pour la mise en œuvre de la gestion des identités.

La troisième partie (ISO-24760 A framework for identity management - Part 3 : Practice) qui est également en cours de rédaction détaillera la mise en pratique de l'architecture définie dans la seconde partie de la norme.

4.1.2 ISO-2700x

Les normes 2700x sont une famille de normes traitant de la sécurité de l'information où la gestion des identités et des accès y est évoquée.

- **ISO/IEC 27000:2009 : Information security management systems - Overview and vocabulary**

Publiée en 2009, la norme ISO/CEI 27000 présente les concepts qui sont manipulés dans les autres normes ISO-2700x. Elle décrit notamment la notion de mesure de sécurité (en anglais : « control ») comme étant un « moyen de gestion du risque, comprenant les politiques, les procédures, les lignes directrices, les pratiques ou l'organisation, qui peuvent être de nature administrative, technique, managériale ou juridique ». Le système de management de la sécurité de l'information (SMSI) est présenté comme une « partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information ». Le processus de qualité PDCA (en anglais : « Plan-Do-Check-Act/Adjust » ; en français : « Planifier-Déployer-Contrôler-Agir/Ajuster ») y est présenté brièvement.

- **ISO/IEC 27001:2005 : Information security management systems – Requirements**

Publiée en 2005, la norme ISO/IEC 27001 définit les exigences pour mettre en œuvre, documenter, exploiter et faire évoluer un SMSI dont le modèle cyclique PDCA est le support. Cette démarche itérative est composée de quatre étapes. La phase de planification concerne la conception du SMSI. La phase de déploiement correspond à la réalisation de ce qui a été planifié. La phase de contrôle permet de vérifier qu'il n'existe pas d'écart entre ce qui a été

planifié et ce qui a été implémenté. La phase d'action permet de corriger les écarts constatés lors de l'étape précédente.

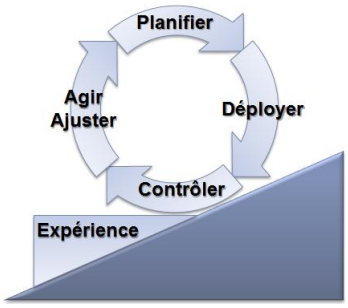

Figure 11 - Processus itératif PDCA de la norme ISO-27001

- **ISO/IEC 27002:2005 : Code of practice for information security management**

Publiée en 2005, la norme ISO/IEC 27002 est un recueil de bonnes pratiques sur la sécurité de l'information. Elle propose un ensemble de mesures de sécurité organisationnelles et techniques, mais aucune solution technique. Le chapitre 11 expose notamment des mesures consacrées à la gestion des identités et des accès dans le but de maîtriser l'accès à l'information (cf. annexe 2 « ISO-27002 – chapitre 11 ») [14]. La politique de contrôle des accès inclut des exigences par exemple autour des « profils d'accès utilisateur normalisés pour les rôles courants au sein de l'organisme » ou de l'« annulation de droits d'accès ». Le sous-chapitre 11.2 décrit les mesures relatives à la gestion de l'accès utilisateur, dont l'enregistrement des utilisateurs, des privilèges et des mots de passe.

- **ISO/IEC 27003:2010 : Information security management system - implementation guidance**

Publiée en 2010, la norme ISO/IEC 27003 contient un guide pratique de mise en œuvre du SMSI suivant le processus PDCA et respectant les exigences de la norme ISO-27002.

- **ISO/IEC 27004:2009 : Information security management system – Measurement**

Publiée en 2009, la norme ISO/IEC 27004 fournit des métriques permettant d'évaluer le niveau d'efficacité du SMSI et par conséquent le niveau de sécurité de l'organisation.

- **ISO/IEC 27005:2011 : Information security risk management**

Publiée en 2008 et révisée en 2011, la norme ISO/IEC 27005 contient un guide de gestion du risque. Elle repose sur les concepts en sécurité de l'information définis par la norme ISO/IEC 27001.

- **ISO/IEC 27006:2011 : Requirements for bodies providing audit and certification of information security management systems**

Publiée en 2009 et révisée en 2011, la norme ISO/IEC 27006 est un recueil d'exigences à destination des organismes qui procèdent à l'audit et à la certification ISO 27001.

- **ISO/IEC 27007:2011 : Guidelines for information security management systems auditing**

Publiée en 2011, la norme ISO/IEC 27007 est un recueil d'instructions pour l'audit et la certification ISO 27001 d'un SMSI.

[14] *ISO/CEI 27002:2005(F)*. ISO/IEC, 130 pages, 2005

- **ISO/IEC 27008:2011 : Guidelines for auditors on information security controls**

Publiée en 2011, la norme ISO/IEC 27008 est un recueil d'instructions à destination des auditeurs accrédités pour vérifier la qualité d'implémentation des mesures de sécurité décrites dans la norme ISO 27002.

4.2 Démarche projet orientée gestion des identités et des accès

L'objectif d'un projet de gestion des identités et des accès est de gérer les utilisateurs et leurs habilitations afin d'arriver à déterminer qui a le droit d'accéder à quoi. La difficulté de ce type de projet évoquée lors des retours d'expérience réside dans la complexité des systèmes d'information existants qui ne permettent pas de construire un ensemble cohérent d'informations. En effet, les informations sont réparties dans de nombreux référentiels. De ce fait, il n'existe aucun moyen d'établir aisément la relation entre identité et habilitations et d'identifier les profils métiers ou les rôles applicatifs. C'est pourquoi il est conseillé d'établir au préalable une cartographie qui prend en compte tous les systèmes d'information permettant de recueillir des informations sur les personnes, les comptes utilisateurs, les profils métiers, les rôles ainsi que les ressources auxquels ils accèdent.

La cartographie doit permettre de mettre en évidence des besoins. L'étape suivante consiste donc à fixer les priorités tant au niveau du système d'information global qu'au niveau fonctionnel. Les différents niveaux de priorité vont définir les objectifs que le système de gestion des identités et des accès devra atteindre. Chaque besoin doit être associé à un responsable ou une maîtrise d'ouvrage métier qui devient alors un des commanditaires, appelé sponsor, du projet. La gestion des identités ayant un impact sur les processus liés aux ressources humaines, au moins en tant que consommateur des informations, un responsable doit donc être impliqué au plus tôt dans le projet.

Une difficulté supplémentaire évoquée lors des retours d'expérience de projets de gestion des identités est une durée trop importante qui est responsable de la diminution de l'implication des équipes fonctionnelles. Lors de projets qui suivent des démarches séquentielles (cf. annexe 3 « Gestion de projet »), le manque de visibilité sur l'avancement du projet peut démotiver les clients du projet. C'est pourquoi les cabinets de conseil et d'intégration préconisent de suivre une méthode itérative avec des livrables visibles à chaque étape.

La démarche préconisée est donc proche des modèles Agiles (cf. annexe 3 « Gestion de projet »). Chaque itération, d'une durée n'excédant pas un mois, doit permettre de livrer un composant de la gestion des identités et des accès auquel sera associé un sponsor correspondant au product owner des méthodes Agiles.

Les différentes étapes s'inscrivent dans un schéma à long terme reposant sur trois phases.
La première phase consiste à bâtir une base solide pour les services de gestion des identités et des accès. Ce socle repose sur la connaissance des associations compte-identité. Pour cela il est nécessaire de nettoyer et mettre en cohérence les différents systèmes et de mettre en place un identifiant unique personnel.
La seconde phase est le déploiement des services de gestion des identités et des accès. Elle intègre la formalisation et l'automatisation des processus de gestion des habilitations. Elle a pour objectif d'offrir un moyen de gérer les accès et d'en réaliser un audit et de produire des rapports.

La dernière phase doit fournir une gestion fine des rôles. Elle débute par une réconciliation des rôles et des accès afin de déterminer qui accède à quelle application, à quel compte, selon quelle règle et avec quels privilèges. L'objectif est de fournir un moyen de gérer intuitivement cet ensemble d'information.

5. Glossaire

ABAC, 21, 25, 26
ACL, 22
Agilité, 32, 40, 46
Attribut, 2, 3, 6, 7, 16, 18, 25, 26
Authentification, 4, 5, 7, 9, 10, 13, 16, 19, 51
Autorisation, 1, 15, 16, 18, 19, 22, 25, 26, 51
Bâle, 27, 28
  Bâle I, 27
  Bâle II, 27
  Bâle III, 28
Cartographie, 32
CIL, 15
Claim, 3
CNIL, 14, 15
Compte, 16, 17, 19, 24, 26, 32, 33, 50, 51
  Compte d'administration, 16
  Compte de service, 16
  Compte global, 16
  Compte utilisateur, 16, 17, 18, 19, 22, 24, 32, 40, 47
Confidentialité, 1, 14, 17
Consommateur d'identité, 4
Contrôle d'accès, 17
CRBF, 28
Credentials *Voir* Justificatif d'identité
Crystal, 46
DAC, 22
Disponibilité, 17
Domaine d'identité, 4, 7, 8, 9, 10, 12
Entité, 2, 3, 10, 12, 16, 17, 18, 19, 22, 26
Feature Driven Development, 46
Fédération d'identité, 4, 8, 13
Fournisseur d'identité, 4, 5, 7, 8, 10, 13
Fournisseur de service, 3, 4, 7, 8, 9, 10, 11, 13, 16
Gestion des identités et des accès
  Gestion des accès, 16, 26, 27, 30
  Gestion des identités, 4, 5, 7, 19, 27, 30, 32
Groupe, 16, 17, 18, 19
Habilitation, 17, 18, 19, 22, 23, 24, 25, 26, 32, 50
IBAC, 21, 22, 23, 25, 26
Identifiant, 3, 7, 8, 9, 10, 12, 16, 27
  Identifiant de référence, 3
  Identifiant unique personnel, 3, 12, 32
  Méta-identifiant, 12
Identification, 3, 7, 9, 10, 19, 28, 39, 51
Identité, 1, 2, 3, 4, 5, 7, 8, 16, 19, 21, 22, 25, 30, 32
  Cycle de vie, 4
  Identité centralisée, 13
  Identité fédérée, 8, 9, 10
  Identité isolée, 10
  Méta-identité, 11, 12
IdP *Voir* Fournisseur d'identité
Incrément, 46
Intégrité, 1, 17, 19, 25, 50
Itération, 25, 32, 44, 46, 47
Iteration planning, 46
Justificatif d'identité, 3, 7, 10, 12, 16
Label, 22
Loi de sécurité financière, 28
MAC, 22, 26
Mêlée, 46
Mesure de sécurité, 30, 31
MLS, 22
NIST, 24
Niveau
  Niveau courant, 23
  Niveau d'habilitation, 22, 23, 26, 51
  Niveau de classification, 23
  Niveau de sécurité, 7, 19, 22, 31
OrBAC, 21, 25, 26
PDCA, 30, 31
Périmètre, 16, 17, 18, 21, 50, 51
  Périmètre fonctionnel, 18
  Périmètre géographique, 18
  Périmètre temporel, 18
Product backlog, 46
Product owner, 32, 46
Profil, 16, 17, 18, 19, 25, 26, 31, 32, 41
Prototype, 44, 45
RBAC, 21, 23, 24, 25, 26
  Constrained RBAC, 24
  Hierarchical RBAC, 24
    General Hierarchical RBAC, 24
    Limited Hierarchical RBAC, 24
  Role engineering, 24
  Rolemining, 24
Ressource, 1, 2, 3, 5, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 32
Rôle, 16, 17, 18, 19, 21, 23, 24, 25, 26, 31, 32, 33, 41, 43, 50

RP *Voir* Consommateur d'identité
RuBAC, 23
Sarbanes-Oxley, 25, 27, 28
Scrum, 46
Segregation of Duty *Voir* Séparation des responsabilités
Séparation des responsabilités, 24, 27, 28
  Séparation dynamique, 24
  Séparation statique, 24
SMSI, 30, 31
SP *Voir* Fournisseur de service
Sponsor, 32, 48
Sprint, 46, 47
Sprint backlog, 46, 47
Sprint planning, 46
Sprint review, 47
SSO, 13
Synchronisation, 12, 47, 50
Test Driven Development, 42, 47
User story, 46
Utilisateur, 4, 7, 8, 9, 10, 12, 13, 16, 18, 22, 23, 24, 25, 31, 32, 40, 46, 50
XP, 46

6. Bibliographie

6.1 Références documentaires

[1] M.R. Nami, A. Malekpour. Virtual Organizations: Trends and Models. Dans IFIP International Federation for Information Processing, Volume 288; *Intelligent Information Processing IV*, Zhongzhi Shi, E. Mercier-Laurent, D. Leake, pages 190–199, 2008

[2] J. Magiera, A. Pawlak. Security Frameworks for virtual organizations. Dans *Organizations: Systems and Practices*. Springer, pages 133-148, 2005

[3] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope. Trust Requirements in Identity Management. *Australasian Information Security Workshop 2005* volume 44, pages 99-108, 2005

[4] *ISO/IEC 24760-1:2011(E)*. ISO/IEC, 20 pages, 2011

[5] E. Bertino, K. Takahashi. *Identity Management: Concepts, technologies and systems*. Artech House, 194 pages, 2010

[6] A. Balat, R. Bergeron, A. Butel, M. Cottreau, F. Depierre, G. Khouberman, L. Mourer, W. Poloczanski. *Gestion des identités*. CLUSIF, 63 pages, 2007

[7] G. Harry. *Failles de sécurité des applications Web*. CNRS, 38 pages, 2012

[8] D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli. *Role-Based Access Control, Second Edition*. Artech House, 381 pages, 2007

[9] F. Cuppens, N. Cuppens-Boulahia. Les modèles de sécurité. Dans *Sécurité des systèmes d'information, (Traité IC2, série Réseaux et télécoms)*. Hermès, pages 13-48, 2006

[10] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security* v.4 n.3, pages 224-274, 2001

[11] M. Frank, J. M. Buhmann , D. Basin. On the definition of role mining. Dans *Proceeding of the 15th ACM symposium on Access control models and technologies*, pages 35-44, 2010

[12] L. Wang, D. Wijesekera, S. Jajodia. A logic-based framework for attribute based access control. Dans *Proceedings of the 2004 ACM workshop on Formal methods in security engineering*, pages 45-55, 2004

[13] G. Chamoret, F. Chavoutier, M. Copitet, J-P Godard, P. Grassart, J. Mauferon, L. Mourer, T. Ramard, G. Remy. *La réforme BÂLE 2, une présentation générale*. CLUSIF, 28 pages, 2004

[14] *ISO/CEI 27002:2005(F)*. ISO/IEC, 130 pages, 2005

[15] L. Audibert. *UML 2 de l'apprentissage à la pratique*. Ellipses, 298 pages, 2009

[16] W. W. Royce. Managing the Development of Large Software Systems : concepts and techniques. Dans *Proceedings of the 9th international conference on Software Engineering*, pages 1-9, 1970

[17] J. McDermid, K. Ripken. Life cycle support in the Ada environment. *ACM SIGAda Ada Letters*, v.III n.1, pages 57-62, 1983

[18] K. Beck. *Test Driven Development: By Example*. Pearson Education, 240 pages, 2002

[19] B. W. Boehm. A Spiral Model of Software Development and Enhancement. *ACM SIGSOFT Software Engineering Notes*, Volume 11 n.4, pages 14-24, 1986

[20] A. Cockburn. *Agile software development*. Addison-Wesley Longman Publishing Co., 278 pages, 2002

6.2 Références Internet

- Bearing Point. *Améliorer la gestion de l'identité et des droits, quels gains pour une DRH ?*, disponible sur : http://blogrh.bearingpoint.com (consulté le 23/04/2012)
- CLUSIF. *Club de la Sécurité de l'Information Français*, disponible sur : http://www.clusif.asso.fr (consulté le 25/04/2012)
- ITFACTO. *Conformité des accès : Identités, annuaire, SSO*, disponible sur : http://www.guidescomparatifs.com/Conformite_des_acces_identites_annuaire_mot_de_passe.asp (consulté le 10/08/2012)
- Identropy. *The Identropy Blog*, disponible sur : http://www.identropy.com/blog/ (consulté le 24/04/2012)
- ISO. *We're ISO, the International Organization for Standardization. We develop and publish International Standards.*, disponible sur : http://www.iso.org (consulté le 25/04/2012)
- Agence Nationale de le Sécurité des Systèmes d'Information. *Portail de la sécurité informatique*, disponible sur : http://www.securite-informatique.gouv.fr (consulté le 25/04/2012)
- Agence Nationale de le Sécurité des Systèmes d'Information. *Actualités, guides, publications*, disponible sur : http://www.ssi.gouv.fr (consulté le 25/04/2012)

Source des icônes libres de droits d'utilisations : http://findicons.com

Annexe 1. ISO 24760 (Table des matières)

FOREWORD ..... **IV**

INTRODUCTION ..... **V**

1 SCOPE **1**

2 NORMATIVE REFERENCES **1**

3 TERMS AND DEFINITIONS **1**

3.1 General terms 1
3.2 Identification 3
3.3 Authenticating an identity 4
3.4 Management of identity 5
3.5 Federation 6
3.6 Privacy protection 7

4 SYMBOLS AND ABBREVIATED TERMS **8**

5 IDENTITY **8**

5.1 General 8
5.2 Identity information 9
5.3 Identifier 10

6 ATTRIBUTES **10**

6.1 General 10
6.2 Types of attribute 11
6.3 Domain of origin 11

7 MANAGING IDENTITY INFORMATION **12**

7.1 General 12
7.2 Identity lifecycle 12

8 IDENTIFICATION **14**

8.1 General 14
8.2 Verification 15
8.3 Enrolment 15
8.4 Registration 15

9 AUTHENTICATION **16**

10 MAINTENANCE **16**

11 IMPLEMENTATION ASPECTS **16**

12 PRIVACY **17**

BIBLIOGRAPHY **18**

INDEX OF TERMS **20**

Annexe 2. ISO-27002 (Table des matières - Chapitre 11)

11 CONTROLE D'ACCES 62

11.1 Exigences métier relatives au contrôle d'accès 62
11.1.1 Politique de contrôle d'accès 62
11.2 Gestion de l'accès utilisateur 63
11.2.1 Enregistrement des utilisateurs 64
11.2.2 Gestion des privilèges 65
11.2.3 Gestion du mot de passe utilisateur 65
11.2.4 Réexamen des droits d'accès utilisateurs 66
11.3 Responsabilités utilisateurs 67
11.3.1 Utilisation du mot de passe 67
11.3.2 Matériel utilisateur laissé sans surveillance 68
11.3.3 Politique du bureau propre et de l'écran vide 68
11.4 Contrôle d'accès au réseau 69
11.4.1 Politique relative à l'utilisation des services en réseau 69
11.4.2 Authentification de l'utilisateur pour les connexions externes 70
11.4.3 Identification des matériels en réseau 71
11.4.4 Protection des ports de diagnostic et de configuration à distance 71
11.4.5 Cloisonnement des réseaux 71
11.4.6 Mesure relative à la connexion réseau 72
11.4.7 Contrôle du routage réseau 73
11.5 Contrôle d'accès au système d'exploitation 73
11.5.1 Ouverture de sessions sécurisées 73
11.5.2 Identification et authentification de l'utilisateur 75
11.5.3 Système de gestion des mots de passe 75
11.5.4 Emploi des utilitaires système 76
11.5.5 Déconnexion automatique des sessions inactives 77
11.5.6 Limitation du temps de connexion 77
11.6 Contrôle d'accès aux applications et à l'information 77
11.6.1 Restriction d'accès à l'information 78
11.6.2 Isolement des systèmes sensibles 78
11.7 Informatique mobile et télétravail 79
11.7.1 Informatique mobile et télécommunications 79
11.7.2 Télétravail 80

Annexe 3. Gestion de projet

Un projet de gestion des identités et des accès repose sur l'ensemble des informations sur les personnes et comptes utilisateurs existants et à venir. Dans le cycle de vie du projet, la phase initiale de spécification doit donc prendre en compte les systèmes d'informations actuels ainsi que le besoin de pouvoir augmenter le périmètre avec l'ajout de nouvelles applications de l'organisme ou de certains partenaires.

1. Cycle de vie

L. Audibert [15] rappelle que tout logiciel ou système d'information suit un cycle de vie divisé en cinq étapes dont chacune englobe un ensemble d'activités.
La phase de spécification et d'analyse des besoins permet de définir l'ensemble des besoins auxquels devra répondre le futur système. Il en résulte généralement un document de spécifications issu des dialogues entre les équipes métiers et les équipes de développement.
La phase de conception permet de définir l'architecture générale du produit attendu en se basant sur les spécifications définies précédemment. A l'issue de cette phase un planning général est décidé et une ébauche de l'interface graphique peut être proposée.
La phase de codage est le moment où les équipes de développement produisent le code opérationnel.
La phase de test permet d'examiner et valider la qualité du produit en se basant sur plusieurs critères. Ainsi, les tests d'acception doivent vérifier que le produit répond aux attentes spécifiées lors de la phase de spécifications. Les tests d'intégration permettent de s'assurer que les différents éléments du système produit s'interfacent correctement avec les autres systèmes d'information de l'organisation. Les tests unitaires, qui doivent être rédigés pendant la phase de codage, reflètent le comportement de l'application. Ils permettent également de connaitre quelles portions de code opérationnel ont été testées et sont conformes aux spécifications.
La phase de maintenance a pour but de corriger ou faire évoluer le produit livré.
La mise en production peut être considérée comme une étape intermédiaire. Cette étape consiste à déployer le système dans l'environnement cible et à ouvrir l'accès aux utilisateurs.

Ce découpage de projet peut être géré selon plusieurs modèles dont l'utilisation dépend du type de projet et de la réactivité attendue. Les méthodes dites « classiques » imposent des modèles stricts où les étapes sont clairement définies avec une production importante de documentation, ce qui convient généralement à de gros projets. A l'opposé, les méthodes dites « Agiles » suivent des modèles itératifs orientés d'avantage sur le code opérationnel que sur la documentation, permettant ainsi des livraisons plus fréquentes.

[15] L. Audibert. *UML 2 de l'apprentissage à la pratique*. Ellipses, 298 pages, 2009

2. Cycle en cascade

En 1970, W. W. Royce [16] a publié le modèle en cascade (en anglais : « Waterfall model »). Le projet, proche du mode de gestion des projets industriels, est alors un enchainement linéaire d'étapes avec un retour possible sur les précédentes. Chaque étape se termine à une date prédéterminée par la livraison de documents ou de modules logiciels. De plus, une nouvelle phase ne peut débuter que si la précédente est complétement achevée et validée, ce qui implique que les livrables attendus sont jugés satisfaisants.

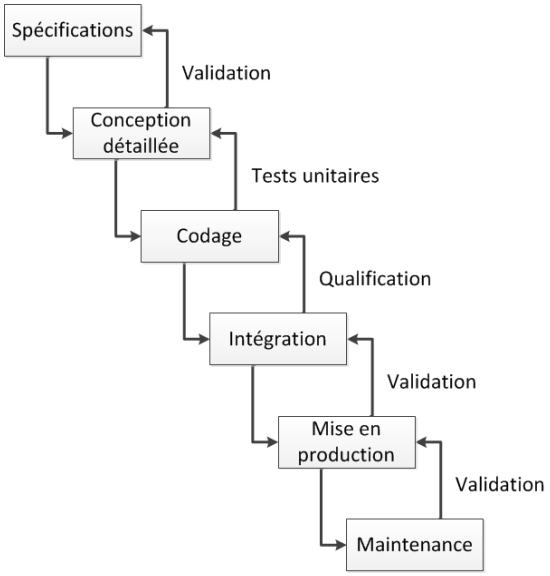

Figure 12 - Cycle de vie de projet en cascade

Ce type de cycle de vie, simple à comprendre et à implémenter, convient aux projets où la qualité a plus d'importance que les coûts ou les délais, et dont les besoins sont clairement définis et stables. Dans le cas contraire, la prise en compte de nouveaux besoins nécessite de dérouler toute la cascade depuis le début. De plus, le client n'est impliqué qu'au début du projet et il ne peut tester le produit qu'à la fin du processus.

Dans le cadre d'un projet de gestion des identités et des accès, les besoins peuvent évoluer. En effet, le déploiement de nouveaux services implique notamment la définition de nouveaux profils ainsi que de nouveaux rôles applicatifs qui doivent être pris en compte, même après la phase de spécification. De ce fait, ce modèle de gestion de projet ne convient pas aux projets de gestion des identités et des accès.

[16] W. W. Royce. Managing the Development of Large Software Systems : concepts and techniques. *Proceedings of the 9th international conference on Software Engineering*, pages 1-9, 1970

3. Cycle en V

En 1983, J. McDermid et K. Ripken [17] ont développé un modèle de cycle de vie pour pallier au manque de réactivité inhérent au modèle précédent. Pour cela, chaque livrable doit être testé pour chacune des étapes. L'omniprésence des tests en parallèle des activités garantit la qualité du produit final. En fonction du jalon, la nature des tests diffère. Ainsi les spécifications sont validées par des tests fonctionnels, également appelés tests de recette, dont le déroulement suit des scénarii décrits dans les documents de spécification. Idéalement, ils sont automatisés, ou réalisés par des personnes indépendantes de l'équipe de développement. Ces tests n'étant exécutés qu'une seule fois à la fin du projet (sauf si le produit livré n'est pas jugé satisfaisant), il serait coûteux de les automatiser.
Les tests d'intégration ont pour but de valider que les développements réalisés s'interfacent correctement avec les systèmes d'information existants.
Les tests unitaires ont pour objectif de vérifier que des portions du code opérationnel se comportent comme le développeur l'a prévu. Pour le développement de ces tests, il est conseillé de suivre le modèle de développement mené par les tests (en anglais : « Test Driven Development ») [18]. Ce processus suit quatre étapes :

1. Ecrire un premier test,
2. Vérifier qu'il échoue (car le code qu'il teste n'existe pas) afin de vérifier que le test est valide,
3. Ecrire le code minimal suffisant pour que le test s'exécute correctement sans erreur,
4. Vérifier que le test n'échoue plus,
5. Améliorer et compléter le code tout en gardant les mêmes fonctionnalités.

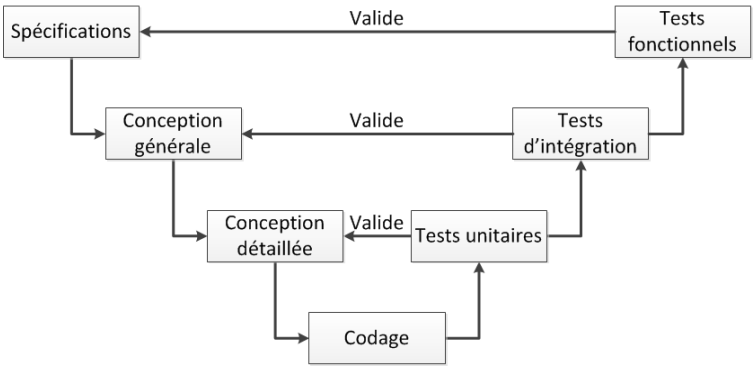

Figure 13 - Cycle de vie de projet en V

A l'instar du modèle en cascade, le modèle en V prend difficilement en charge de nouveaux besoins ou la modification des spécifications. En effet, l'effet tunnel induit par les modèles séquentiels montre qu'une erreur dans la formulation ou l'interprétation des spécifications ne peut être détectée qu'à la fin du cycle. En effet, la maîtrise d'ouvrage n'est impliquée qu'en début et fin de cycle, ce qui peut représenter plusieurs mois d'intervalle pour un gros projet.

Bien que plus nombreuses que dans un cycle en cascade, les possibilités de prise en compte de nouveaux besoins restent faibles. En effet, dans le cadre d'un projet de gestion des identités et des accès, après la phase de spécification, la mise à disposition d'un nouveau service, ne peut être prise en compte qu'au moment des tests d'intégration. De plus, ces changements impliqueraient la remise en cause du travail effectué jusqu'à la phase des tests

[17] J. McDermid, K. Ripken. Life cycle support in the Ada environment. *ACM SIGAda Ada Letters*, v.III n.1, pages 57-62, 1983

[18] K. Beck. *Test Driven Development: By Example*. Pearson Education, 240 pages, 2002

unitaires. L'utilisation de ce type de cycle de vie pour un projet de gestion des identités et des accès implique que l'ajout d'une application, de laquelle découle de nouveaux rôles, impose un projet propre avec le déroulement complet du cycle de vie. De ce fait, ce modèle n'est pas recommandé dans le cas d'un projet de gestion des identités et des accès.

4. Cycle en spirale

En 1988, B. W. Boehm [19] a introduit les notions d'itération et de prototypage dans le cycle de vie d'un projet informatique pour pallier au manque de visibilité inhérent aux démarches séquentielles.

Une itération correspond à l'exécution du cycle de vie pour un sous-ensemble des spécifications qui se conclut par la livraison d'un produit opérationnel. La prise en compte de l'ensemble des spécifications nécessitant plusieurs itérations, l'équipe fonctionnelle du projet dispose régulièrement d'un outil qu'elle peut soumettre à l'ensemble des tests évoqués avec le cycle en V. Cette démarche permet de réajuster régulièrement les spécifications, budgets et délais. Une itération peut prendre en compte des spécifications qui ont déjà fait l'objet d'une itération, ce qui offre une capacité de réaction face à l'évolution des besoins.

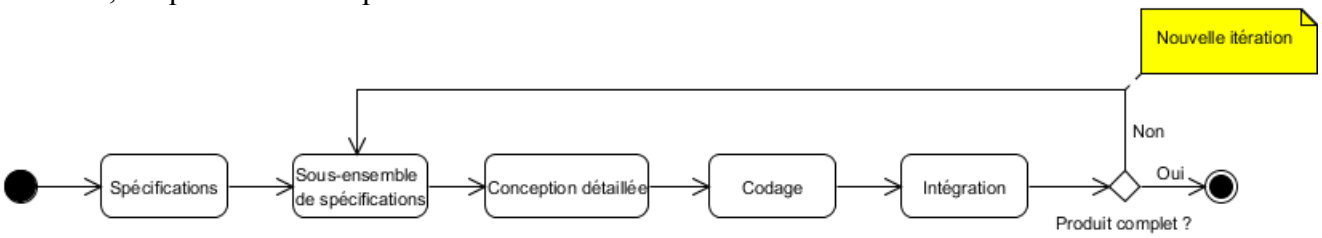

Figure 14 - Diagramme d'activité d'une démarche itérative

Un prototype est une réalisation partielle de l'étape de codage qui simule le comportement d'un sous-ensemble des fonctionnalités attendues. Les règles de codage ne sont alors pas nécessairement suivies. Le prototype n'a pas vocation à être déployé. En effet, le but est que les développeurs soumettent leur compréhension des spécifications. Ce dialogue permet de diminuer les risques en s'assurant à différents jalons du projet que les choix d'implémentation répondent aux besoins des clients du projet. En effet, le prototype est soumis à l'évaluation de l'équipe fonctionnelle du projet et peut subir des modifications jusqu'à ce qu'il soit validé. C'est seulement à partir de cette étape que les activités du projet peuvent continuer.

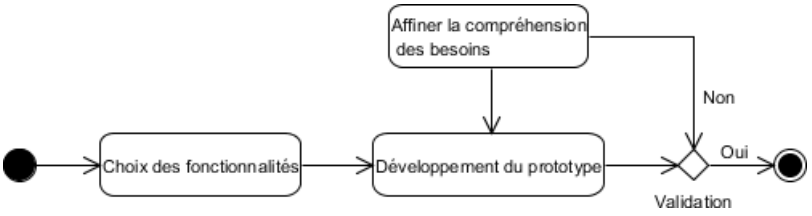

Figure 15 - Diagramme d'activité de réalisation d'un prototype

Le modèle en spirale, proposé par B. W. Boehm, divise le cycle de vie global d'un projet en minimum trois itérations (représentées graphiquement par des spirales) qui suivent chacune un cycle de vie complet composé de quatre phases :

1. Détermination des objectifs à partir de l'analyse des besoins ou du résultat des cycles précédents,
2. Analyse des risques avec une phase dédiée au prototypage,
3. Développements et tests. Dans la dernière spirale il est possible de suivre une démarche séquentielle telle que la cascade ou le V,
4. Validation du résultat puis planification.

[19] B. W. Boehm. A Spiral Model of Software Development and Enhancement. *ACM SIGSOFT Software Engineering Notes*, Volume 11 n.4, pages 14-24, 1986

La première itération de l'analyse des besoins et des risques permet de placer les fonctions critiques dans le premier cycle de prototypage et de développement. Ainsi, les objectifs et les développements à prendre en compte dans les itérations suivantes auront un risque d'impact minimisé sur les itérations antérieures.

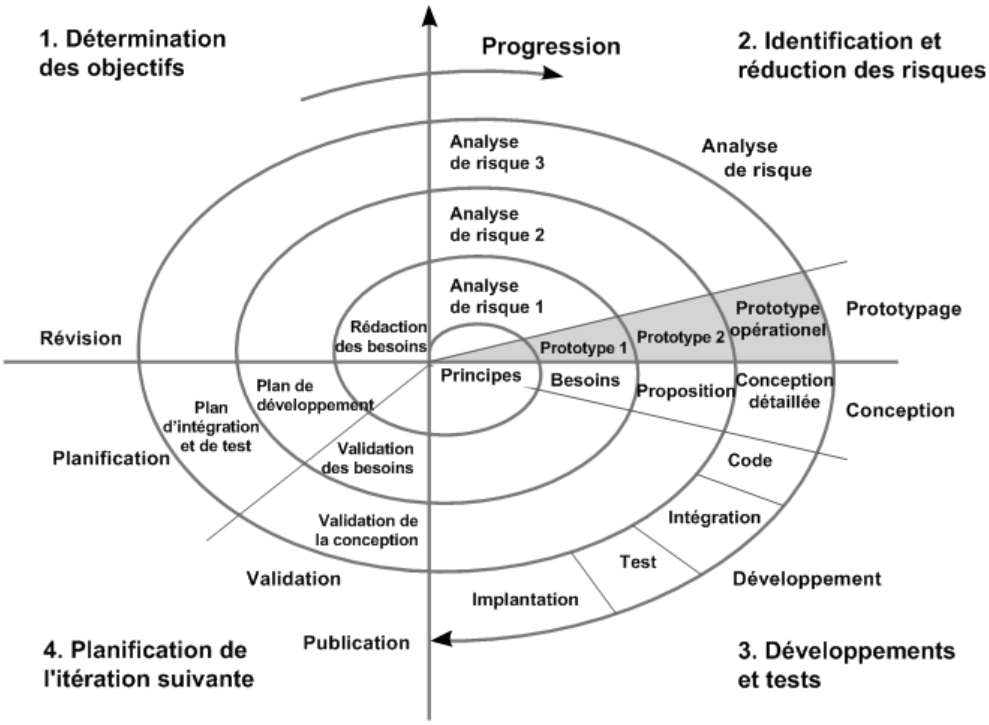

Figure 16 - Cycle de vie de projet en spirale

L'évaluation répétée des besoins, des risques et des développements propre à ce modèle permet de contrôler régulièrement si les délais et budgets seront respectés, contrairement aux démarches séquentielles où ils ne peuvent être vérifiés qu'à l'approche de la date de livraison. De plus, le client du projet est plus impliqué dans la vie du projet que dans les modèles linéaires, où son action est limitée à la phase de rédaction du cahier des charges et à la validation du produit final.

La démarche en spirale permet des interactions plus fréquentes entre les différentes équipes engagées dans un projet par rapport aux modèles linéaires. Cependant, après la phase de spécification, les besoins peuvent être ajustés, mais il n'est pas facile de prendre en compte d'importantes modifications ou ajouts. En effet, ce type de changement implique de reprendre complètement l'analyse de risque qui représente une part important du projet dans le cycle en spirale.

Dans le cadre d'un projet de gestion des identités et des accès, ce type de cycle de vie permet de prendre en compte de nouveaux besoins induits par le déploiement de nouveaux services. Cependant, les possibilités sont limitées. Les spécifications doivent intégrer la capacité de modification du périmètre des applications sans imposer la réalisation d'une nouvelle analyse de risque qui peut être longue et coûteuse. Cette possibilité particulière doit être testée au plus tôt lors de la réalisation d'un prototype. Le cycle de vie itératif semble donc envisageable pour des projets de gestion des identités et des accès. Cependant le cycle de vie en spirale n'est pas le plus adapté à cause des impacts financiers et en délai des analyses de risque.

5. Méthodes Agiles

En 2001, dix-sept experts en développement logiciel se sont réunis pour présenter leurs méthodes (Adaptive Software Development, XP, Scrum, Crystal, Feature Driven Development, Dynamic System Development Method (DSDM) et « pragmatic programming ») [20]. Suite à l'analyse des avantages de chacune de ces méthodes, ils ont extrait quatre valeurs fondamentales et douze principes pour constituer le manifeste des méthodes de développement Agiles (cf. annexe 4 « The Manifesto for Agile Software Development »).

Afin d'obtenir un produit opérationnel répondant aux attentes des utilisateurs, les démarches Agiles reposent sur les quatre règles fondamentales suivantes.

- Les individus et leurs interactions plutôt que les processus et les outils,
- Des logiciels opérationnels plutôt qu'une documentation exhaustive,
- La collaboration avec les clients plutôt que la négociation contractuelle,
- L'adaptation au changement plutôt que le suivi d'un plan.

Pour mettre en pratique ces principes, les méthodes Agiles préconisent un cycle itératif et incrémental incluant notamment les phases de spécification, développement et validation. Par rapport à la démarche en spirale, en Agilité le cycle est complété par la notion d'incrément même si la notion est proche de celle d'itération, dans le cas de l'incrément, le découpage du projet en sous-ensemble ne se fait plus au niveau des spécifications, mais au niveau des composants. Un seul ensemble de composants est développé par incrément. Chaque incrément vient s'intégrer au premier incrément du projet appelé le noyau. La mise en œuvre de cette division des besoins et des composants, se fait au travers de « Sprints ». Le sprint correspond à une étape d'un mois maximum dont les objectifs sont définis dans le carnet du sprint, le « Sprint backlog ». Le sprint backlog spécifie les fonctionnalités qui doivent être développées ou corrigées lors du sprint. Les méthodes agiles ayant pour principe de privilégier la réalisation de code fonctionnel plutôt que la rédaction de documentation technique ou fonctionnelle, cette dernière peut faire l'objet d'un sprint dédié. Par ailleurs, la plus grande partie des fonctions de l'outil est définie en début de projet dans le carnet du produit, le « Product backlog ». Chaque cas d'utilisation est décrit dans une « User story » à laquelle sont affectées une priorité et une estimation du volume de travail nécessaire pour le développer, le tester et le valider.

De plus, les méthodes Agiles prônent la collaboration entre les personnes impliquées dans et par le projet, ce qui requiert notamment l'intégration de la maîtrise d'ouvrage et des utilisateurs au cours du développement. Pour répondre à ces besoins, l'équipe projet inclut un propriétaire du produit (en anglais : « Product owner ») qui est un expert du métier. Il va jouer le rôle du client. Il doit être capable de définir les spécifications fonctionnelles, d'établir la priorité des fonctionnalités à développer ou corriger et valider les fonctionnalités développées.

Afin de favoriser le dialogue, les méthodes Agiles prévoient plusieurs types de réunions qui sont à programmer à différents moments du projet.
Avant chaque sprint, une réunion de planification, le « Sprint planning » ou « Iteration planning », permet de sélectionner dans le product backlog les fonctions à implémenter qui constitueront le sprint backlog en fonction des priorités du client.
Durant le sprint, la « mêlée » permet à l'équipe de se regrouper pendant quinze minutes maximum quotidiennement pour évoquer les problèmes rencontrés dans la journée, éventuellement y assigner des développeurs supplémentaires, mais sans chercher à les

[20] A. Cockburn. *Agile software development*. Addison-Wesley Longman Publishing Co., 278 pages, 2002

résoudre. L'identification des problèmes peut être facilitée par la mise en place d'une plate-forme d'intégration continue. Ce type d'outil permet de compiler, vérifier et tester automatiquement l'ensemble du code opérationnel dès qu'un nouvel élément est publié, ce qui implique de suivre le modèle « Test Driven Development » évoqué précédemment. Cette réunion permet également de vérifier que toutes les user stories du sprint backlog seront terminées à la date de fin prévue de l'itération.
A la fin du sprint, une réunion de rétrospective, la « Sprint review », permet de capitaliser sur les problèmes rencontrés, les solutions mises en œuvre, ainsi que les causes de perte d'efficacité et de qualité. C'est également l'occasion de présenter le résultat du sprint avec la démonstration des nouvelles fonctions ou des corrections.

La mise en œuvre de ces concepts permet d'offrir de la souplesse au projet et de donner de la visibilité au client sur les réalisations.

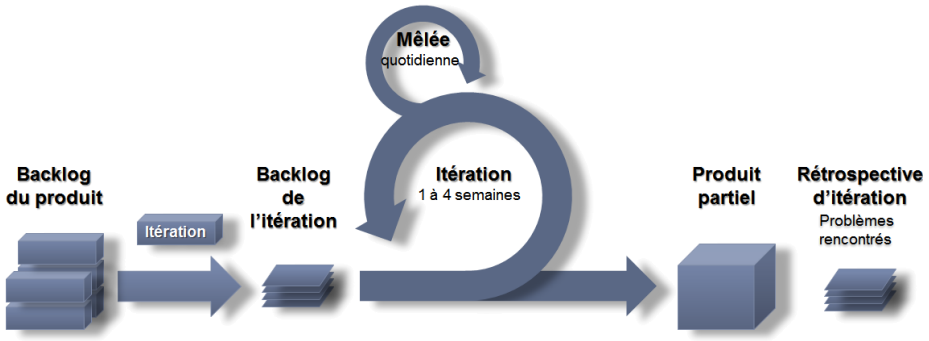

Figure 17 - Cycle de vie en « Agilité »

Cette méthode est applicable pour le développement initial d'un projet mais aussi lors de la maintenance applicative.

Dans le cadre d'un projet de gestion des identités et des accès, la livraison d'itérations simples et successives peut permettre d'assembler les informations sur les personnes et les comptes utilisateurs au fur et à mesure de la prise en compte de nouveaux systèmes d'information. La difficulté de synchronisation entre toutes les applications impactées est alors répartie sur plusieurs itérations. L'évolution des besoins étant la base de ce type de cycle de vie, il convient parfaitement aux projets de gestion des identités et des accès.

Annexe 4. The Manifesto for Agile Software Development

Seventeen anarchists agree:

We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- Individuals and interactions over processes and tools.
- Working software over comprehensive documentation.
- Customer collaboration over contract negotiation.
- Responding to change over following a plan. That is, while we value the items on the right, we value the items on the left more.

We follow the following principles:

- Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.
- Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.
- Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
- Business people and developers work together daily throughout the project.
- Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
- The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
- Working software is the primary measure of progress.
- Agile processes promote sustainable development. The sponsors, developers and users should be able to maintain a constant pace indefinitely.
- Continuous attention to technical excellence and good design enhances agility.
- Simplicity.the art of maximizing the amount of work not done.is essential.
- The best architectures, requirements and designs emerge from self-organizing teams.
- At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

Kent Beck, Mike Beedle, Arie van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, Jon Kern, Brian Marick, Robert C. Martin, Steve Mellor, Ken Schwaber, Jeff Sutherland, Dave Thomas

www.agileAlliance.org

Annexe 5. Grille d'évaluation technique

Les critères de la grille d'évaluation sont issus en partie du cahier des charges de gouvernance des accès mis à disposition gratuitement par la société guidescomparatifs.com.

1. Gestion des identités

Tableau XIII - Grille d'évaluation technique : Référentiel intégré

Critères	Compléments
La solution peut-elle utiliser un référentiel intégré ?	Annuaire LDAP Base de données relationnelle Autre
La solution est-elle compatible SAML ?	Compatible CAS, Shibboleth ?

Tableau XIV - Grille d'évaluation technique : Connecteurs

Critères	Compléments
Quels sont les connecteurs vers d'autres annuaires supportés ?	Active Directory Microsoft Exchange NIS OpenLDAP V3 Autre
Quels sont les connecteurs fichiers supportés ?	Attribute-value pair text files Delimited text file Fixed-width text files LDIF Autre
Quels sont les connecteurs bases de données supportés ?	Microsoft SQL Server Oracle Database MySQL PostgreSQL Autre
Quels sont les autres connecteurs supportés ?	DSML 2.0 SAP Autre
Peut-on développer ses propres connecteurs ?	
La solution permet-elle de détecter des changements dans les sources de données ?	

Tableau XV - Grille d'évaluation technique : Transformation

Critères	Compléments
La solution permet-elle de traiter les données en entrée et en sortie d'un connecteur ?	Concaténation de chaîne Opérations arithmétiques Extraction de chaînes Autre
Quel langage de programmation est supporté pour le traitement des données ?	Perl PHP C, C++ C# Visual Basic C#, .Net XSLT Java JavaScript Autre

Tableau XVI - Grille d'évaluation technique : Provisioning

Critères	Compléments
La synchronisation des informations est-elle gérée par la solution ?	De manière événementielle Nécessite des actions manuelles Autre
La solution permet-elle de créer, supprimer et modifier des entrées dans les applications via les connecteurs ?	
La solution permet-elle de mettre en place un processus de création, modification ou suppression des comptes applicatifs au travers des différents connecteurs (par exemple, création de l'entrée dans l'application de ressources humaines en premier, puis dans Active Directory, puis dans Novell Netware) ?	Par configuration graphique Par programmation au niveau des règles de jointure et de transformation
La solution permet-elle de créer des comptes en masse ?	
La solution permet-elle d'anticiper la création de compte ?	
La solution permet-elle la création de comptes de test ?	
La solution permet-elle de propager les informations rapidement ?	En moins de 30s En temps réel Sur évènement
La solution permet-elle de désactiver temporairement un utilisateur ou un groupe (pas d'authentification possible) ?	Période de désactivation Désactivation d'un utilisateur Désactivation d'un groupe ou d'un rôle Autre

2. Gestion des accès

Tableau XVII - Grille d'évaluation technique : Gestion des rôles

Critères	Compléments
La solution supporte-t-elle des rôles ?	Groupe dynamique Groupe dynamique avec mise à jour automatique d'un attribut pour tous les utilisateurs
La solution permet-elle de renommer les rôles selon un langage métier ?	
La solution permet-elle de prendre en compte la séparation des responsabilités dans la définition des rôles ?	
La solution permet-elle de définir des exceptions à l'intérieur de rôles paramétrés ?	
La solution permet-elle de gérer l'intégrité référentielle (suppression automatique d'un membre d'un groupe en cas de suppression de l'entrée utilisateur associée) ?	

Tableau XVIII - Grille d'évaluation technique : Gestion des habilitations

Critères	Compléments
La solution permet-elle d'envoyer régulièrement aux utilisateurs une revue des utilisateurs sous leur responsabilité, afin de leur faire valider ou invalider les accès de leur équipe ?	Peut-on définir -la fréquence ? -la forme ? -le périmètre ? Autre(s) paramètre(s)
La solution est-elle en mesure de mettre en œuvre des processus d'escalade dans le processus de certification des habilitations ?	Exemple: pour procédure provisoire de délégation lors de l'absence du responsable
La solution produit-elle un reporting sur les revues d'habilitation ?	

Critères	Compléments
La solution permet-elle de générer des alertes ?	Temps donné au processus de certification Niveaux d'habilitations Habilitations exceptionnelles Autre
Lors de l'autorisation d'une personne à accéder à une application, une fonction de workflow est-elle disponible pour informer et faire valider par les personnes habilitées l'autorisation de cet accès ?	

Tableau XIX - Grille d'évaluation technique : Gestion des mots de passe

Critères	Compléments
La solution permet-elle de chiffrer les mots de passe ?	
La solution gère-t-elle l'historique du mot de passe ?	
Si Oui, peut-on paramétrer la limite de l'historique (par exemple, 10 derniers)	
La solution permet-elle de gérer le changement du mot de passe ?	
Si Oui, peut-on forcer le changement du mot de passe à la première connexion ?	
En cas de gestion de mot de passe, peut-on forcer le changement du mot de passe régulièrement ?	
La solution gère-t-elle l'expiration du mot de passe ?	
La solution permet-elle de contrôler le contenu du mot de passe ?	
La solution permet-t-elle le blocage d'un compte en cas d'erreur de mot de passe ?	Nombre de tentatives Délai entre deux tentatives Autre
La solution pert-elle de synchroniser les mots de passe avec Active Directory ?	

Tableau XX - Grille d'évaluation technique : Contrôle et traçabilité

Critères	Compléments
La solution dispose-t-elle de fonctions de traçabilité ?	Peut-on définir -la fréquence ? -la forme ? -le périmètre ? Autre(s) paramètre(s)
Quels sont les événements couverts par le module de traçabilité ?	Authentification Gestion de mot de passe Workflow d'approbation Modification de rôle Autre
Quel est le mode de gestion du module de supervision/traçabilité ?	Traçabilité passive Gestion d'événement / réactivité sur événement
Dans le cas d'une gestion réactive sur événement, quel est le périmètre couvert par le déclenchement d'action ?	Par exemple 3 échecs d'identification + 1 réussite sur 1 minute peuvent laisser supposer une tentative d'intrusion
Quelles sont les actions possibles déclenchées par le module de supervision actif ?	Envoi de mail Déconnexion d'accès Autre
La solution dispose-t-elle de modèles de rapports prédéfinis ?	