LES DOSSIERS TECHNIQUES

Gestion et Gouvernance des Identités et des Accès

Guide pratique – Mise en œuvre

Février 2017

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

Remerciements

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

Le responsable du groupe de travail :

Olivier	MOREL	***ILEX International***

Les contributeurs à la rédaction de ce document :

Stéphane	CAMOUS	***ICF Habitat***
Delphine	de SAINT CYR	***BOURSE DIRECT***
Zahi	DIB	***IDENTO***
Rémi	FOURNIER	***SYNETIS***
Benoît	FUZEAU	***CASDEN BANQUE POPULAIRE***
Patrick	MARACHE	***WAVESTONE***

Ainsi que tous les membres ayant participé aux nombreuses sessions du groupe de travail,

et en particulier :

Mohamed BAKKALI (***ANSSI***); Valérie CHASSAING (***PSA Groupe***) ; Rachid ELOUARGHANI (***MODIS***) ; Florence HANCZAKOWSKI (***CLUSIF***) ; Astrid LANG (***AP-HP***) ; Alice MILANOVA (***MAIF***) ; Sylvain MOREAU (***DEXIA***) ; Sven NEUBERT PAJADON (***BETA SYSTEMS***); Christiane PAYAN (***ORANGE***) ; Manuel PRIEUR (***Hewlett Packard Enterprise***) ; Emmanuelle SELOSSE (***IMPRIMERIE NATIONALE***) ; Eric THIERRY (***MANUTAN International***) ; André SONNOIS (***EDENRED***)

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture de ce document.

I. Introduction

I.1. Description du sujet

En juillet 2007, le CLUSIF a publié un dossier technique intitulé « Gestion des identités », disponible en téléchargement sur son site Internet. Si les concepts fonctionnels et techniques exprimés dans ce dossier restent évidemment bons, il y manque aujourd'hui de nombreux éléments, du fait des évolutions du marché de la sécurité informatique au sens large, et de celle de la gestion des identités et des accès :

- évolution des usages et des technologies : Cloud/SaaS, Mobilité, …
- évolution des approches de mise en œuvre : approche par les risques ou par la gouvernance des identités et des accès, approche itérative…
- évolution des contraintes : législation, cybercriminalité, …
- etc.

En 2015, le CLUSIF a souhaité produire un nouveau dossier sur « la Gestion et la Gouvernance des Identités et des Accès » (Identity & Access Management (IAM) / Identity & Access Governance (IAG)), en s'appuyant sur les nombreux retours d'expériences de ses adhérents. Il ne s'agissait pas de revoir ou corriger le document de 2007, mais bien d'en préparer un nouveau, organisé différemment, et plus orienté sur des « cas d'usages » concrets.

Le nouveau groupe de travail (GT) avait ainsi initialement pour ambition de produire un document abordant tous les concepts associés à la Gestion et à la Gouvernance des Identités et des Accès et à destination de tous : interlocuteurs techniques ou fonctionnels, décideurs ou utilisateurs.

Lors de nombreux ateliers de travail, le GT a beaucoup partagé autour de cas d'usages concrets, de retours d'expériences d'implémentation, et de bonnes pratiques autour de l'IAM/IAG.

Le parti retenu a été de livrer un « **guide pratique d'implémentation de projets IAM/IAG** », en identifiant notamment, pour tous les domaines fonctionnels et techniques qui composent l'IAM/IAG, l'ensemble des prérequis techniques et organisationnels, conseils pratiques ainsi que des points d'attention à prendre en compte avant, pendant ou après un tel projet.

Notre ambition est ainsi d'être le plus pragmatique possible, et de retranscrire dans ce livrable les expériences et conseils de ceux qui ont déjà mis en œuvre ce type de projets.

I.2. A qui s'adresse ce document ?

Ce document d'adresse à toute personne en charge d'initier ou de mettre en œuvre tout ou partie d'un projet d'IAM/IAG dans son organisation : DSI, RSSI, chef de projet, architecte, MOA, MOE, consultant, etc.

I.3. Profil des participants au GT

Le GT s'est tenu sur environ deux années, au rythme moyen d'une séance d'échanges et de travail mensuelle. Trente personnes y ont participé au moins une fois, de façon plus ou moins active, avec la répartition suivante :

- 2/3 d'« utilisateurs » : tous secteurs d'activités, toutes tailles d'entreprise ;
- 1/3 d'« offreurs » : cabinets de conseil, intégrateurs, éditeurs.

I.4. Objectifs du document

L'objectif principal de ce document est d'aider à l'appropriation et à la mise en œuvre d'un projet de gestion et de gouvernance des identités et des accès. Il vise à présenter des éléments simples et pragmatiques afin de mieux appréhender son projet et ainsi de réduire le risque d'échec.

Le GT a ainsi décidé de présenter un document sous la forme d'un guide méthodologique agrémenté de bonnes pratiques, en étant le plus pragmatique possible, en s'appuyant sur les expériences de ses membres.

Nous avons souhaité organiser le document en suivant les phases du cycle de vie d'un projet d'IAM, en se positionnant ainsi :

- avant le projet ;
- pendant le projet ;
- après le projet.

Constatant que les projets d'IAM ne s'implémentent plus dans une logique de « Big Bang » mais plutôt par une succession d'itérations ou de lots, nous avons également choisi de considérer un projet d'IAM « global » comme un ensemble de sous-projets de mise en œuvre de « briques de l'IAM ».

Le document est ainsi composé de différents modules fonctionnels pouvant être pris séparément selon la typologie des sujets à traiter ou les préoccupations rencontrées.

I.5. Ce qui n'est pas traité dans ce document …

Dans l'esprit décrit ci-dessus, il a fallu faire des choix pour privilégier un document efficace et utile. Certains sujets ont ainsi été volontairement écartés, pour différentes raisons : soit il s'agit de sujets trop récents ou pas assez matures sur le marché français, donc pauvres en retours d'expériences, soit il s'agit de sujets qui peuvent être traités de manière totalement indépendante de l'IAM/IAG.

Le GT n'a donc pas ou peu traité des sujets tels que l'IAM de l'Internet des Objets, le « Customer IAM », l'IAM « as a Service », le Contrôle d'Accès Physique ou encore la gestion des comptes à privilèges.

Le GT s'est concentré sur les sujets d'IAM les plus fréquemment rencontrés, privilégiant une approche pragmatique de mise en œuvre plutôt qu'une approche théorique ou dogmatique.

Enfin, ce document ne présente aucune solution du marché du fait de l'existence de nombreux rapports d'analystes sur ce sujet en particulier.

I.6. Acronymes

Les différents acronymes utilisés dans le document sont présentés ci-dessous. Un glossaire en annexe du présent document fournit également des définitions pour l'ensemble des notions évoquées dans le document.

Acronymes	Signification
2FA	Two Factor Authentication
ABAC	Attribute Based Access Control
ACL	Access Control List
AD	Active Directory
ADFS	Active Directory Federation Services
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
BYOD	Bring Your Own Device
B2B	Business To Business
B2C	Business To Consumer
CAPEX	Capital Expenditure (dépenses d'investissement)
CAS	Central Authentication Service
CIAM	Customer Identity & Access Management ou Consumer Identity & Access Management
CMS	Card Management System
COPE	Corporate Owned, Personally Enabled
CPE	Carte de Personnel d'Établissement
CPS	Carte de Professionnel de Santé
CLUSIF	CLUb de la Sécurité de l'Information Français
CNIL	Commission Nationale de l'Informatique et des Libertés
CYOD	Choose Your Own Device
DSI	Directeur des Systèmes d'Informations
GDPR	General Data Protection Regulation ou RGPD pour Règlement Général sur la Protection des Données
GRC	Governance, Risk management & Compliance
IAG	Identity & Access Governance

IAI	Identity Analytics & Intelligence
IAM	Identity & Access Management ou GIA pour Gestion des Identités et des Accès
IAMaaS	Identity & Access Management as a Service
IDaaS	Identity as a Service
IdP	Identity Provider
IGA	Identity Governance and Administration
IHM	Interface Homme Machine
IoT	Internet of Things
IRM	Identity Relationship Management
ITSM	Information Technology Service Management
eIDAS	electronic IDentification And trust Services
eSSO	enterprise Single Sign-On
FAQ	Foire Aux Questions
FIDO	Fast IDentity Online
GT	Groupe de Travail
LDAP	Lightweight Directory Access Protocol
LPM	Loi de Programmation Militaire
LSF	Loi de Sécurité Financière
MCO	Maintien en Condition Opérationnelle
MFA	Multi-Factor Authentication
MOA	Maîtrise d'OuvrAge
MOE	Maîtrise d'Œuvre
NFC	Near Field Communication
OIDC	OpenID Connect
OIV	Opérateur d'Importance Vitale
OOB	Out-Of-Band
OPEX	Operational Expenditure (dépenses d'exploitation)
ORBAC	Organisation Role Based Access Control
OTP	One-Time Password
PaaS	Platform as a Service

PAM	Privileged Account Management
PIM	Privileged Identity Management
PUM	Privileged User Management
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure ou IGC pour « Infrastructure de Gestion de Clés »
POC	Proof-Of-Concept (démonstrateur)
PSSI	Politique de Sécurité des Systèmes d'Information
RBAC	Role Based Access Control
RFID	Radio Frequency IDentification
RGS	Référentiel Général de Sécurité
ROI	Return On Investment (Retour Sur Investissement)
RSSI	Responsable de la Sécurité des Systèmes d'Information
SAAS	Software As A Service
SAML	Security Assertion Markup Language
SI	Système d'Information
SIEM	Security Information and Event Management
SP	Service Provider
SPOF	Single Point of Failure
SoD	Segregation of Duty
SOX	Sarbanes-OXley
SLO	Single Log Out
SSO	Single Sign-On
TMA	Tierce Maintenance Applicative
UBA	User Behaviour Analytics
UEBA	User & Entity Behaviour Analytics
WAM	Web Access Management

II. Principes fondamentaux de l'IAM et de l'IAG

Ce chapitre vise à donner une définition simplifiée des principes fondamentaux couverts par la Gestion et la Gouvernance des Identités et des Accès. En effet, les terminologies sont nombreuses (IAM, IAG, IGA, IRM, IAI, IDaaS…) et ne fournissent pas toutes une vision claire de ce qu'elles recouvrent.

Aussi, nous avons retenu de présenter une vision simple – et simplifiée – de l'IAM/IAG en regroupant les principes fondamentaux autour de 6 enjeux concrets :

1. améliorer et simplifier la gestion des identités, des droits et des comptes ;
2. piloter, auditer et contrôler les identités, les droits et les accès ;
3. authentifier les utilisateurs ;
4. contrôler et simplifier l'accès aux applications ;
5. étendre les services IAM/IAG et IAI ;
6. tirer parti du cloud.

II.1. Améliorer et simplifier la gestion des identités, des droits et des comptes

Il s'agit ici de simplifier et d'automatiser les actions du quotidien liées à la gestion des identités et de leurs droits.

II.1.1. Gestion du cycle de vie des identités

La gestion du cycle de vie des identités consiste à modéliser et outiller la gestion des événements de la vie d'une identité au sein de l'entreprise.

Elle couvre ainsi :

- toutes les populations devant se connecter au SI de l'entreprise : employés, prestataires in situ et ex situ, fournisseurs, partenaires, clients… voire demain des objets connectés, les machines, les robots, etc. ;
- tous les événements touchant à une identité au cours de son cycle de vie et pouvant varier selon les populations et selon les activités : arrivée, changement de poste, départ, arrivée/retour de saisonnier, détachement, absence longue durée, suspension, mission supplémentaire, etc.

Pour cela, il est nécessaire de :

- prendre en compte les référentiels maîtres déjà présents dans l'entreprise (SI-RH pour les internes en général, bases spécifiques ou applications des achats pour les prestataires ou les partenaires, référentiels organisationnels, etc.) via des alimentations régulières ;
- offrir des IHM et des processus de gestion (workflows d'approbation) pour les populations ou les événements sans référentiel maître, comme par exemple les prestataires ;
- permettre de configurer des contraintes dans la gestion de certaines populations comme :
  - la possibilité de limiter les personnes autorisées à créer des prestataires ;
  - la saisie obligatoire de la date de fin de mission pour les prestataires ou les personnels sous contrat à durée déterminée, avec suspension automatique de leurs comptes sur le SI à cette date ;
  - des campagnes de revue périodiques pour confirmer par exemple la présence des prestataires ou les missions d'un employé.

II.1.2. Gestion des habilitations

Les identités étant gérées, il convient également de gérer leurs habilitations sur le SI, c'est-à-dire leur(s) compte(s) applicatif(s) et leurs droits dans les applications.

La gestion des habilitations s'appuie généralement sur :

- un **modèle d'habilitation**, c'est-à-dire la modélisation homogène des droits sur le SI ;
- une **organisation « back office »** en charge de la définition et de l'évolution de cette modélisation ;
- des **processus d'approbation** en cas de demande, modification ou retrait d'un droit ;
- une **organisation « front office** » en charge d'approuver, de rejeter ou de compléter les demandes soumises.

Enfin, pour simplifier l'expérience utilisateur et faire de l'IAM l'outil principal de la gestion des demandes, la gestion des habilitations peut être étendue à d'autres ressources comme :

- des badges d'accès logique ou physique : restauration, machine à café, etc. ;
- des équipements IT : téléphone portable, tablette, etc. ;
- des droits d'accès physiques : accès aux bâtiments, à certains locaux, etc.

II.1.2.a. Le modèle d'habilitation

La modélisation des habilitations doit être compréhensible par les demandeurs. Pour cela elle doit être « orientée métier » et cohérente avec la maturité de l'entreprise. Il n'existe donc pas une « unique bonne modélisation » des habilitations, même s'il existe des principes ou des théories de modélisation comme les modèles ABAC, RBAC, ORBAC, etc.

Les modèles les plus simples se limiteront à quelques profils applicatifs, voire uniquement à l'autorisation (oui/non) à une application.

De manière plus courante, des modèles d'habilitations plus évolués combinent, selon les besoins et la maturité de l'organisation, les notions suivantes :

- des **profils métiers** décrivant une responsabilité dans les processus de l'entreprise. Ils regroupent un ou plusieurs profils applicatifs. A titre d'exemple, dans un hôpital, le profil métier « radiologue » regroupera des profils applicatifs « médecin » pour l'accès au dossier médical et « radiologue » pour l'accès aux images et à la saisie des comptes rendus dans le système d'imagerie médicale ;
- des **profils applicatifs** associés à une application, au sens métier du terme et non technique. A titre d'exemple, un module d'un ERP peut être considéré comme une application à part entière car il représente un ensemble cohérent de privilèges sur cette application pour réaliser une tâche ;
- une notion de **périmètre ou portée** décrivant un périmètre de données sur lequel va s'appliquer un profil métier ou applicatif. Les périmètres peuvent être construits sur une arborescence comme par exemple un pays, une région, un site, un bâtiment, un service.

Enfin, les modèles les plus matures possèdent des fonctionnalités avancées comme :

- **l'attribution automatique de profils** sur la base des attributs du bénéficiaire. Cette automatisation reste néanmoins l'apanage des organisations très matures et relativement stables, sans cas d'exceptions, comme par exemple : les points de ventes ou les entrepôts dans le secteur de la grande distribution, ou encore les agences dans le secteur bancaire ;
- la **suggestion de profils** sur la base des attributs du bénéficiaire. Cette suggestion reste une indication pour aider le demandeur dans sa requête. Par exemple, quand 90% des personnes ont un profil calculable à partir de leur métier ou diplôme, une validation de la suggestion automatique - avec ajustement possible le cas échéant - est rapide et évite les erreurs ;
- des **règles de conflits,** ou matrice d'incompatibilité, entre différents profils (*SoD*), ou entre un profil et les attributs du bénéficiaire. Ces règles permettent, par exemple, d'éviter qu'une même personne puisse créer et valider une action sensible comme passer un virement bancaire ;
- une date de début et de fin pour l'attribution des profils.

II.1.2.b. L'organisation « back office »

Elle est en charge de faire vivre le modèle d'habilitation dans le temps :

- suivi des usages : profils non attribués, profils attribués systématiquement et pouvant être automatisés, profils ajoutés fréquemment, etc. ;
- prise en compte de l'évolution du SI : nouvelles applications, nouvelles fonctionnalités dans une application, nouveaux déploiements, etc. ;
- prise en compte de l'évolution de l'organisation.

Pour ce faire, elle pourra s'appuyer sur des fonctionnalités du décisionnel appliquées à l'IAM/IAG, à savoir sur les principes d'IAI (Identity Analytics & Intelligence) décrits ci-après.

II.1.2.c. Les processus d'approbation

Les processus d'approbation doivent permettre de valider – ou non - la légitimité d'une attribution ou d'une modification de droits. Ils sont déclenchés lors de la demande, de la prolongation ou de la suppression d'un droit, mais également en cas de mobilité interne du bénéficiaire, de demande de droit sensible, etc.

Quatre natures d'approbations sont généralement utilisées dans ces processus :

- **hiérarchique** : par le manager, le responsable d'entité ;
- **fonctionnelle** : par un référent du profil ou de l'application demandée ;
- **sécurité** : en cas de droit ayant un impact significatif en termes de risque ;
- **budgétaire** : dans une optique de maîtrise ou de réduction du coût des licences.

Pour viser des processus efficaces, il convient idéalement de ne pas dépasser deux étapes d'approbations dans la majorité des situations.

La définition d'un nombre fini et limité de processus d'approbation assure la maintenabilité de la solution. Idéalement, l'utilisation de profils métiers ou applicatifs permet de choisir automatiquement le processus à suivre.

II.1.2.d. L'organisation « front office »

L'organisation « front office » est en charge de la soumission des demandes de droits, de leur approbation ou refus. Cette organisation doit être :

- cohérente avec l'organisation de l'entreprise ;
- au plus près des utilisateurs pour être en mesure d'évaluer la légitimité des demandes.

La tendance actuelle est de permettre aux utilisateurs de soumettre des demandes pour eux-mêmes en mode self-service, voire pour tout autre utilisateur. Ce fonctionnement nécessite de porter une attention renforcée à l'ergonomie de la solution et à la définition des profils métiers et applicatifs.

Enfin, pour des populations spécifiques, comme les partenaires notamment, une partie de cette gestion peut être déléguée. Là encore, la délégation exige une responsabilisation forte et contractualisée.

II.1.3. Provisioning

Après avoir géré les demandes d'habilitations, il reste à créer les comptes et droits ad hoc sur le SI. C'est l'objectif du provisioning. Il cherche à maintenir à jour les référentiels majeurs comme l'annuaire Active Directory et les annuaires LDAP ainsi que les référentiels propres à chaque application.

Plusieurs niveaux d'intégration sont possibles.

Le **provisioning automatique** vise à créer automatiquement les comptes et droits nécessaires. Techniquement, il est nécessaire d'implémenter des connecteurs, des web-services ou autres solutions. Fonctionnellement, il faut s'assurer que les règles ayant conduit à l'automatisation restent valables dans le temps. Il est important de souligner que le provisioning applicatif n'est possible qu'avec le concours en amont de l'éditeur de l'application, et que des limites du provisioning peuvent apparaître dans ce cadre.

Le **provisioning manuel** ou **guidé** nécessite que les actions techniques soient réalisées manuellement par un administrateur. Pour le mettre en œuvre, il existe principalement deux approches :

- interfacer l'outil IAM/IAG avec l'outil ITSM existant. Ainsi, l'IAM/IAG crée un ticket dans l'ITSM puis suit son traitement afin de pouvoir afficher un niveau d'avancement à l'utilisateur ;
- implémenter directement dans l'IAM les processus appropriés pour notifier les administrateurs des tâches en attente et leur permettre de rendre compte de leurs actions.

Le **provisioning mixte** ou **semi-automatique** combine des tâches automatiques et des actions manuelles. Suivant le contexte, il permet de combiner plusieurs avantages tels que :

- la gestion automatique des attributs sensibles comme le statut actif ou suspendu d'un compte ou le délai d'expiration des mots de passe afin de garantir un haut niveau de sécurité ;
- la gestion manuelle des droits d'accès pour une implémentation simple.

Le **provisioning « à la volée »**, est apparu plus récemment avec les outils de fédération d'identités. Il consiste à fournir, dans le jeton d'identité échangé, l'ensemble des informations nécessaires à la création et à la mise à jour du compte. Charge alors à l'application consommant ce jeton de créer le compte à la première connexion de l'utilisateur puis de le mettre à jour lors des accès suivants.

II.2. Piloter, auditer et contrôler les identités, les droits et les accès

L'objectif est ici de disposer de la capacité à piloter, auditer et contrôler les accès au SI. Historiquement ces fonctions étaient relativement peu développées dans les solutions d'IAM, jusqu'à l'apparition d'outils dédiés à cet enjeu, sous le nom d'IAG ou IAI (Identity & Access Governance, Identity Analytics & Intelligence). A noter qu'à ce jour les outils d'IAM cherchent à étendre leur couverture fonctionnelle, menant parfois à un recouvrement entre solutions d'IAM, d'IAG et d'IAI.

Les solutions IAM, IAG et IAI se distinguent par:

- **la conception intrinsèque des outils** : les outils d'IAI sont le pendant « Business Intelligence » de l'IAM. Ils sont construits autour d'un puits de données ou cube de données et ont vocation à réagir a posteriori ;
- **la granularité des droits gérés** : les outils d'IAM et d'IAG se limitent en grande majorité aux droits dont ils doivent gérer l'attribution. Par exemple dans SAP, il s'agira des rôles composites. Allant plus loin, les outils d'IAI ont vocation à recréer la chaîne de liaison complète, jusqu'au droit le plus fin dans les applications. Par exemple dans SAP, il s'agira des transactions. L'objectif est de détecter les risques ou les non-conformités dues à la définition des rôles ou des profils.
- **Les sponsors et donneurs d'ordre visés** : les solutions d'IAI visent en premier lieu à maîtriser le niveau de risques liés aux droits d'accès. En ce sens, elles s'adressent prioritairement aux directions des risques et à l'audit interne.

Ainsi, et de manière très schématique, l'IAI vise principalement 3 objectifs :

- **améliorer la qualité des données** par des contrôles de cohérence et une assistance à l'identification des sources d'incohérence ;
- **maîtriser les risques liés aux habilitations** avec un suivi de l'attribution des droits à risques, le pilotage de campagnes de revues et la gestion des exceptions ;
- **ajuster le modèle d'habilitation** ou « Role Management » grâce à l'analyse de l'usage des profils métiers et applicatifs définis et à la comparaison des droits attribués et transactions effectivement utilisées.

L'intérêt de l'IAI prend toute sa dimension lorsque les directions des risques et de l'audit interne sont fortement impliquées dans le projet.

La suite du chapitre donne un éclairage rapide sur les principales fonctionnalités d'un IAI.

II.2.1. Puits de données (ou cube de données)

Véritable cœur de la solution, le puits de données a vocation à :

- stocker et archiver toutes les données importées ;
- organiser ces données dans un modèle partagé (ou pivot).

L'intérêt de ce modèle est de pouvoir simplement étendre la solution IAI à de nouvelles ressources, sans remettre en question les tableaux de bord et autres traitements construits sur ce modèle partagé.

II.2.2. Brique d'alimentation

La brique d'alimentation permet d'alimenter le puits de données. Pour cela, elle doit :

- être compatible avec le maximum de sources et de formats ;
- offrir des fonctionnalités d'amélioration de la qualité des données : vérification des règles de format, détection des doublons ou d'enregistrements proches ;
- prendre en considération les comptes avec leurs droits tout autant que les traces d'accès afin de pouvoir ensuite comparer les droits donnés avec les droits réellement utilisés.

II.2.3. Fonctionnalités d'analyse et d'alerte

Sur la base du modèle partagé du puits de données, les fonctionnalités d'analyse et d'alerte permettent d'implémenter les indicateurs, alertes et tableaux de bord propres au contexte client. Par exemple :

- règles de cohérence des données : comptes d'employés non présents dans le SI RH, ou présents dans plusieurs systèmes, utilisateurs avec des comptes applicatifs mais sans compte AD, etc. ;
- règles de cohérence de droits d'accès : un utilisateur de la Direction Marketing ayant accès à des transactions ou à un répertoire partagé du Département Financier, un utilisateur d'un service hospitalier ayant accès à d'autres hôpitaux avec un profil ne correspondant pas à son métier, etc. ;
- règles de séparation de tâches (SoD) : un utilisateur possédant des rôles toxiques, un profil métier présentant un risque intrinsèque, etc.

II.2.4. Brique de revues ou recertification et interface utilisateur

La brique de revues ou de recertification a vocation à paramétrer et piloter des campagnes de revues sur les identités et sur les comptes. Elle se découpe en trois phases qui sont :

- l'organisation de la campagne : périmètre à couvrir, utilisateurs concernés, fréquence de la campagne, acteurs responsables ;
- le suivi et le pilotage de la campagne : suivi des réponses, relances, redirections vers de nouveaux acteurs ;
- la clôture de la campagne et la génération des preuves.

À cette brique de revues, s'ajoutent les interfaces utilisateurs permettant de suivre les indicateurs paramétrés, effectuer une recherche ou une vérification.

II.3. Authentifier les utilisateurs

Authentifier un utilisateur vise à garantir, avec un niveau de confiance adapté, son identité. L'objectif de ce chapitre est de donner un aperçu des moyens d'authentification autres que le simple couple « login/mot de passe » encore très répandu.

II.3.1. Authentification forte, authentification renforcée, MFA

Sans qu'il existe de définition officielle et partagée, **l'authentification forte** peut se définir comme la combinaison de deux principes :

- la combinaison d'au moins deux facteurs différents parmi les suivants :
  - ce que je sais et que je suis le seul à connaître : par exemple un mot de passe ou un code PIN ;
  - ce que je possède : par exemple une carte à puce, un certificat, un token ou un smartphone ;
  - ce que je suis : par exemple par une empreinte digitale, un réseau veineux, un visage.
- au moins un de ces facteurs n'est pas rejouable. C'est-à-dire que les données échangées entre l'utilisateur et le serveur ne peuvent pas être réutilisées. Ainsi, même si elles sont interceptées, elles restent inutilisables.

Traditionnellement la notion d'**authentification renforcée** est utilisée lorsque le caractère non rejouable n'est pas assuré.

Depuis quelque temps, c'est le terme « **MFA** » ou « 2FA » qui est utilisé pour définir cette authentification multi-facteurs. Cependant, malgré le caractère « fort » de ce type d'authentification, il reste des attaques auxquelles ces authentifications restent sensibles comme le Man-In-The-Middle ou le Phishing.

Pour sécuriser encore plus l'authentification, des mécanismes complémentaires sont envisageables. Les principaux sont décrits dans la suite du chapitre.

II.3.2. Authentification OOB (Out-Of-Band)

L'authentification OOB consiste à recourir, pour un facteur d'authentification, à un canal différent de celui utilisé pour accéder à l'application.

- Exemple OOB : accès à une application Web à partir d'un PC + application sur un smartphone recevant une notification *push* dans laquelle il faut confirmer son identité.
- Exemple non OOB : accès à une application Web à partir d'un PC + envoi d'un SMS sur un smartphone, à ressaisir dans l'IHM de l'application Web.

II.3.3. Biométrie comportementale

La biométrie comportementale consiste à comparer le comportement de l'utilisateur par rapport à son « empreinte comportementale ». Cette dernière peut être générée lors d'une phase d'enrôlement ou construite progressivement, à mesure que l'utilisateur utilise ses équipements.

A titre d'exemples : la vitesse ou la dynamique de frappe, les mouvements de la souris, les habitudes dans l'utilisation d'un écran tactile.

II.3.4. Risk based authentication, adaptive authentication

Le principe de l'authentification basée sur les risques est de s'appuyer sur des « indices » de confiance pour évaluer si le comportement constaté correspond au comportement « classique » de l'utilisateur ou relève « d'une situation à risque ». A titre d'illustration :

- la détection de l'usage d'un nouvel équipement, par exemple un nouveau PC ;
- la détection d'une tentative d'accès inhabituelle, par exemple à partir d'un pays étranger, ou sur une plage horaire remarquable ;
- la détection d'une navigation non conforme dans l'application, par exemple une tentative de saisie d'un virement bancaire sans consultation préalable du solde du compte ;
- l'utilisation de la biométrie comportementale.

Sur la base de ces facteurs de risques, chaque application pourra implémenter un comportement adapté comme par exemple :

- ne pas en tenir compte et poursuivre la navigation ;
- poursuivre la navigation mais notifier l'utilisateur par mail ou marquer la transaction comme étant « à risque » dans le back-office ;
- demander une nouvelle preuve d'authentification, éventuellement forte ou différente ;
- bloquer la fonctionnalité demandée.

II.4. Contrôler et simplifier l'accès aux applications

L'objectif ici est double :

- simplifier l'accès de l'utilisateur en limitant les demandes d'authentification : c'est le principe du SSO qui vise, après une première authentification, à ne plus authentifier l'utilisateur durant une période déterminée ;
- contrôler l'accès aux applications, c'est-à-dire vérifier que l'utilisateur est bien autorisé à réaliser l'accès demandé, et tracer cet accès.

Pour parvenir à cet objectif, il existe plusieurs approches techniques, qui visent des situations différentes. Les solutions associées s'appuient sur des référentiels d'identités et assurent l'audit et la traçabilité des authentifications et des habilitations. Elles fournissent également des fonctionnalités de contrôle d'accès logique et sont généralement couplées à des technologies d'authentification forte.

II.4.1. eSSO ou Entreprise SSO

Le eSSO consiste à agir à la place de l'utilisateur. Son composant « cœur » est le moteur eSSO qui est en charge de :

- détecter des fenêtres applicatives, comme par exemple des fenêtres d'authentification, d'erreur d'authentification, de changement de mots de passe ;
- remplir à la place de l'utilisateur les champs nécessaires à l'authentification, en général le login et le mot de passe et éventuellement des champs complémentaires.

Il est nécessaire pour cela que :

- un administrateur ait configuré au préalable les fenêtres à détecter par la solution eSSO, ainsi que les différents comportements attendus par la solution ;
- le eSSO connaisse les « accréditations secondaires » de l'utilisateur pour cette application, c'est à dire son couple login / mot de passe. Ceci peut être réalisé de deux manières différentes :
  - par auto-apprentissage : à sa première connexion, le eSSO demande à l'utilisateur de saisir, pour la dernière fois, son login et son mot de passe ;
  - par provisioning via un outil d'IAM/IAG capable d'alimenter automatiquement le eSSO, qui doit, par exemple, fournir une API pour cela.

Les solutions de eSSO peuvent également offrir des fonctionnalités avancées telles que :

- le changement automatique du mot de passe sur l'application ;
- les traces consolidées des accès ;
- la détection de mots de passe partagés par plusieurs utilisateurs ;
- la délégation d'un utilisateur à un autre.

Les solutions de eSSO présentent les avantages :

- de ne pas être intrusives par rapport aux applications couvertes en ne nécessitant pas de modifications dans l'application ;
- d'être compatibles avec un très grand nombre d'applications clients lourds ou clients légers.

En revanche, elles présentent les inconvénients :

- d'être généralement adhérentes au poste de travail par l'installation du moteur eSSO et de ne pouvoir donc être déployées que sur des postes maîtrisés ;
- de s'exécuter du côté poste de travail et non du côté serveur applicatif ce qui peut générer une charge de déploiement et de support supplémentaire ;
- de nécessiter une éventuelle reconfiguration lors d'évolutions des applications du périmètre.

II.4.2. WebSSO, ou Web Access Management (WAM)

Les solutions de WebSSO/WAM sont nées avec l'explosion des applications en mode client léger. Elles s'appuient sur des tickets de session, à l'image de Kerberos dans le monde Microsoft.

Aussi, une solution de WebSSO/WAM doit :

- générer des tickets de session ce qui nécessite la mise en œuvre d'une infrastructure centrale en charge de cette opération;
- contrôler la validité du ticket lors de l'accès d'un utilisateur à une ressource protégée par le WebSSO/WAM. Un composant de contrôle dans la chaîne d'accès entre l'utilisateur et l'application doit alors être installé, soit directement sur le serveur de l'application – il s'agit alors d'un « agent » - soit sur un reverse proxy en amont de l'application.

Étant positionnées en rupture de flux entre l'utilisateur et l'application, les solutions de WebSSO/WAM apportent un niveau de sécurité supérieur aux solutions de eSSO. Elles offrent les avantages suivants :

- les mots de passe ne sont potentiellement plus stockés dans les référentiels des applications, à part pour certaines applications qui l'imposent ;
- les règles de contrôle d'accès peuvent être implémentées de manière centralisée. Par exemple interdire l'accès à une ressource hors des heures ouvrées, imposer une authentification forte ou supplémentaire ;
- des profils d'accès plus fins peuvent être définis pour un utilisateur donné, permettant de limiter les fonctionnalités ou les transactions accessibles à cet utilisateur ;
- la traçabilité, notamment des authentifications et des autorisations, est assurée ;
- elles ne sont pas intrusives vis-à-vis du poste de travail et peuvent être déployées sur des environnements pour lesquels les postes de travail ne sont pas maîtrisés ;
- elles s'exécutent côté infrastructure, ce qui assure généralement un niveau de fiabilité supérieur.

En revanche, ces solutions présentent les inconvénients suivants :

- n'être compatibles qu'avec les applications Web et être potentiellement intrusives sur ces applications si des adaptations sont nécessaires pour des raisons de compatibilité ;
- être un SPOF, ce qui nécessite de mettre en place une infrastructure hautement disponible ainsi qu'une organisation et un processus appropriés.

Toutefois, les standards de Fédération d'Identités tendent à s'étendre aussi aux solutions de WebSSO/WAM, et donc à simplifier l'intégration avec les applications modernes.

II.4.3. Fédération d'Identités

La Fédération d'Identités peut être vue comme l'évolution du WebSSO/WAM pour suivre deux transformations SI majeures :

- l'ouverture du SI à des populations extérieures non gérées directement par l'entreprise ;
- le Cloud Computing et l'accès à des ressources externes non gérées directement par l'entreprise.

Pour répondre à ces deux transformations, la Fédération d'Identités s'appuie sur l'échange de jetons d'identité et définit deux principes fondateurs :

- s'appuyer sur des standards partagés et reconnus comme par exemple *SAMLv2, OAuth2, OpenIDConnect, WS-Federation* ;
- standardiser et séparer les responsabilités de Fournisseurs d'Identités (IdP) de celles de Fournisseurs de Services (SP).

À titre d'illustration :

Cas d'une entreprise accédant à un service Cloud :

- l'entreprise s'appuie sur sa gestion des identités : elle joue le rôle de Fournisseur d'Identités ;
- elle accède à un service extérieur : il joue le rôle de Fournisseur de Services.

Cas d'une entreprise mettant à disposition un portail partenaire pour ses fournisseurs ou ses clients :

- l'entreprise joue le rôle de Fournisseurs de Services vis-à-vis de ses fournisseurs ;
- les fournisseurs assurent le rôle de Fournisseurs d'Identités.

La Fédération d'Identités peut également proposer des fonctionnalités avancées comme :

- le provisioning à la volée pour créer et maintenir à jour les comptes des utilisateurs. En revanche, la suppression des comptes n'est pas toujours assurée ;
- l'« impersonnalisation », c'est-à-dire le fait de partager des informations entre IdP et SP tout en garantissant un certain anonymat de l'accédant.

Par exemple, une entreprise se connectant à un portail fournisseur peut fournir comme information :

- l'identifiant de l'entreprise ;
- le profil d'accès de l'utilisateur.

Ainsi l'entreprise ne communique pas de données à caractère personnel des utilisateurs.

Les solutions de Fédération d'Identités présentent les avantages :

- d'être un standard de fait dans le monde Internet et de s'étendre aux applications Web en général ;
- de traiter un très grand nombre de cas d'usages ;
- de permettre de désactiver de façon centralisée les accès aux applications fédérées.

En revanche, elles affichent les inconvénients :

- de nécessiter une relation de confiance, généralement matérialisée contractuellement, entre l'IdP et le SP ;
- de posséder une faiblesse dans la maîtrise de la traçabilité des accès. L'IAI permet cependant de pallier ce manque.

II.4.4. Mobile SSO

Le Mobile SSO vise à offrir un service de SSO sur les périphériques mobiles tels que les smartphones et les tablettes. C'est le domaine le plus récent investi par le SSO. Aussi, les normes sont encore jeunes et les solutions assez rares. Il convient cependant de relever l'émergence du standard OAuth2 for Native Apps dont l'objectif est de fournir des fonctionnalités de SSO entre les applications mobiles.

Ce standard se décline suivant l'OS mobile :

- BrowserView pour iOS ;
- Custom Tab pour Android.

Ce standard a pour but de demander aux applications natives, équivalentes à des clients lourds, de s'appuyer sur le navigateur du système pour gérer l'authentification et le SSO. Il est même envisageable d'utiliser ce principe pour obtenir un SSO sur un poste de travail classique entre les applications Web et les clients lourds.

II.5. Étendre les services IAM/IAG et IAI

II.5.1. Sécuriser les comptes administrateurs à hauts privilèges

Les comptes administrateurs du SI, à hauts privilèges, présentent des particularités techniques : comptes non personnels, comme les comptes « root », fonctionnalités spécifiques, comme les commandes « sudo », etc. Leur sécurisation nécessite donc une approche et des moyens particuliers.

C'est l'objectif d'outils spécifiques dénommés parfois PIM, PUM ou encore PAM. Ces outils se trouvent la plupart du temps « en dehors » de la solution IAM/IAG, mais sont couplés avec celle-ci, ou au moins l'AD. Ils s'appuient par exemple sur le principe de bastion de sécurité en se positionnant « en coupure » entre l'administrateur et le système à administrer :

- l'administrateur s'authentifie et accède à ce bastion de sécurité ;
- il réalise ses actions d'administration au travers de ce bastion ;

Le bastion apporte des fonctionnalités avancées : gestion des accès des administrateurs, trace des accès, enregistrement de session, mise à jour des mots de passe des comptes à privilèges, etc.

II.5.2. Sécuriser les données non structurées

La sécurisation des données non structurées, telles que les répertoires partagés, présentent des particularités techniques. En effet :

- c'est souvent la donnée elle-même qui porte les autorisations. Par exemple, les ACL portent sur un fichier ou un répertoire. Les autorisations ne sont donc pas centralisées, ou portées par les comptes d'accès, mais sont distribuées sur chaque donnée non structurée à protéger : répertoire partagé, fichier, espace de stockage Cloud, espace SharePoint, etc. ;
- le volume des données non structurées dans une entreprise est gigantesque, y compris pour les entreprises de taille modeste. Les études estiment que 80% des données d'une entreprise sont non-structurées ;
- la nature des données non structurées est très variée : personnelle, financière, commerciale, R&D, de santé, relative à des moyens de paiement, etc. ce qui multiplie les réglementations à respecter ;
- les données non structurées sont extrêmement volatiles, créées en « temps réel ».

Aussi, pour couvrir les données non structurées, le prérequis indispensable est de définir un cadre, une politique, d'accès à ces données.

De manière courante, cette politique :

- normalise les bonnes pratiques et donc limite les granularités autorisées et la finesse d'autorisations possibles ;
- tente d'interdire les autorisations directes au profit d'autorisations données à des groupes de comptes pour une gestion plus centralisée : ce ne sont pas les comptes qui ont des autorisations sur les données mais des groupes de comptes qui ont les autorisations sur les données.

Une fois ce cadre posé, et pour aider à son déploiement, les solutions doivent notamment offrir les capacités suivantes :

- reconstruire de bout-en-bout la chaîne d'autorisation de la donnée au compte d'accès ;
- justifier des raisons conduisant à un accès autorisé ou non. Par exemple l'appartenance à un groupe, à une direction métier ou autorisation unitaire ;
- analyser les usages, mettre en lumière des usages s'éloignant de ceux les plus couramment constatés et alerter si nécessaire ;
- remédier de manière automatique à une illégitimité.

En matière d'outillage, deux approches sont envisageables.

- Utiliser des solutions dédiées à la couverture des ressources non structurées : ces solutions peuvent être des modules supplémentaires de solutions IAM/IAG ou des solutions totalement autonomes. Elles offrent généralement l'avantage de proposer un niveau d'intégration très poussé avec les technologies couvertes. En revanche, elles sont généralement limitées à quelques technologies ou types de ressources et peuvent ainsi créer un effet « silo » ne permettant pas une analyse transverse au niveau de l'entreprise.
- S'appuyer sur des modules IAM/IAG et IAI déjà déployés. Ces deux modules se partagent les responsabilités : le module IAM/IAG assure la gestion des demandes d'accès et le provisioning jusqu'à un groupe d'accès. Il offre les fonctionnalités d'*analytics* pour reconstruire la chaîne d'autorisation de bout-en-bout et s'assurer que seuls les groupes d'accès sont autorisés sur les données non structurées, sans gérer d'autorisation unitaire.
  Sans nécessiter de modules supplémentaires, cette approche offre l'avantage de proposer une vision transverse des autorisations sur les applications et les données non structurées, quelle que soit la technologie sous-jacente. Elle permet donc de faire des analyses sans être prisonnier d'un « silo ».
  En revanche, elle impose l'application stricte de la politique, en imposant le passage systématique par un groupe d'accès. De plus, si une non-conformité est détectée sur une ressource, par exemple l'attribution d'une autorisation directe sans passer par un groupe, la solution d'IAI pourra lever une alerte. Cependant, dans la plupart des cas, elle ne saura pas corriger cet écart et une action complémentaire, souvent manuelle, sera nécessaire.

II.5.3. Analyser les comportements

Les solutions IAI les plus innovantes commencent à offrir des fonctionnalités d'analyse des comportements. Elles sont fréquemment appelées UBA pour *User Behaviour Analytics* ou UEBA pour *User & Entity Behaviour Analytics*.

Leur promesse est de détecter des comportements à risques ou *a minima* des comportements qui divergent de l'usage « courant » constaté. Pour cela, ces fonctionnalités ne s'appuient pas sur des règles *a priori* ou des schémas prédéfinis. Au contraire, elles mettent en jeu des technologies innovantes de type *Big Data* ou *Machine Learning* pour :

- consolider les traces applicatives produites par chaque application ;
- analyser et corréler ces traces entre-elles et par rapport aux caractéristiques des identités ;
- identifier, sur la base de modèles mathématiques, des comportements qui diffèrent de la « moyenne des comportements constatés ».

Il est ensuite nécessaire d'analyser unitairement les écarts détectés pour séparer les vrais usages inappropriés des faux-positifs.

Ces fonctionnalités avancées peuvent être utilisées, en particulier, en cas de lutte contre la fraude. Elles peuvent également permettre d'aider à la compréhension des usages réels sur le terrain, et ainsi adapter et améliorer les fonctionnalités IAM, comme par exemple les processus, le modèle d'habilitation, etc. Dans un second temps, elles pourront également être rapprochées des services de SIEM, encore souvent limités aux événements réseau et IT et loin des logiques applicatives et métier.

II.6. Tirer parti du cloud

Les services d'IDaaS/IAMaaS visent à offrir les fonctionnalités d'IAM dans le Cloud, c'est-à-dire en mode SaaS.

Comme pour les autres services IT, nombreux sont les clients qui s'interrogent sur la pertinence de recourir au Cloud pour les services IAM. A la date de rédaction de ce document, le recours à ces services reste limité car toutes les briques IAM n'offrent pas le même niveau de maturité :

- les services Cloud associés à la gestion des accès, tels que l'authentification multi-facteurs, le SSO ou la Fédération d'Identités, offrent déjà un niveau de maturité intéressant ;
- les services Cloud associés à la gestion des identités restent en retrait par rapport à l'offre « on-premise ». A noter que la couverture fonctionnelle n'est pas nécessairement identique chez un même éditeur offrant sa solution en mode « on-premise » et en mode Cloud ;
- les services Cloud associés à l'IAI sont les moins bien représentés dans les offres Cloud.

Les approches les plus répandues actuellement sont au mieux « hydrides », combinant une infrastructure « on-premise » et certains services Cloud.

Enfin, pour pallier le manque d'offres Cloud, certains intégrateurs tendent à délivrer des implémentations de solutions « on-premise » sur des hébergements Cloud (PaaS). Ce mode de délivrance reste lui aussi assez récent et n'offre pas un niveau de service identique à une offre Cloud à part entière.

III. Pourquoi démarrer un projet IAM/IAG ?

Dans le chapitre précédent nous avons proposé de regrouper les principes de l'IAM/IAG autour de 6 enjeux concrets qui mettent en évidence un certain nombre de composants ou modules. Cela étant, dans ce document, et comme précisé au chapitre I.5, nous n'avons volontairement pas abordé en détail l'ensemble des briques fonctionnelles de l'IAM/IAG, privilégiant les modules les plus fondamentaux, les plus répandus et les plus matures sur le marché actuel, rassemblés par « grandes familles ».

La représentation graphique de la Gestion et la Gouvernance des Identités et des Accès pouvant se présenter sous différentes formes, nous avons fait le choix d'une représentation classique correspondant à l'organisation du présent document.

Note :

Nous aurions pu faire d'autres choix dans la mesure où les flèches « Gestion des Accès » et « Gestion des Identités » pourraient tout à fait se rejoindre au milieu de la section « annuaire d'identités », puisqu' il faut bien un référentiel d'Identité pour les deux domaines.

De même, ne pas mettre la flèche « gouvernance » en recouvrement sur la partie « Gestion des Identités » pourrait laisser penser qu'il n'y a pas de dimension métier dans la gouvernance, ce qui n'est évidemment pas le cas.

Il y a également des fonctions de revues des habilitations dans la gestion des identités, et nous aurions pu tout aussi bien positionner uniquement deux flèches : une pour la « Gestion des Accès », et une englobant les parties « Gestion des Identités » et « Gouvernance », que nous aurions nommée par exemple « Identity Administration & Governance ».

Les motivations liées au démarrage de tout ou partie d'un projet de Gestion et Gouvernance des Identités et des Accès sont nombreuses. C'est pourquoi l'objet de ce chapitre n'est pas d'en dresser la liste exhaustive mais plutôt d'identifier de nombreux cas d'usages ou objectifs concrets qui sont autant d'arguments justifiant de lancer un projet d'IAM/IAG.

Le tableau ci-après présente un certain nombre de ces cas d'usages, organisés par domaines fonctionnels et problématiques, en face desquels nous avons positionné les briques de l'IAM/IAG les plus directement concernées.

La liste n'est pas exhaustive, d'autres cas d'usages sont fournis dans la suite du document, et notamment dans les fiches pratiques présentées au chapitre VI.

Domaines	Exemples de problématiques et de cas d'usages	Auth. forte	SSO	Fédération	Annuaire	Cycle de vie	Habilitations	Revues	Rôles
Sécurité	Savoir qui peut accéder à quoi								
	Savoir qui accède à quoi								
	Supprimer l'utilisation de mots de passe triviaux et adapter le niveau d'authentification au contexte								
	Contrôler et tracer les accès aux applications depuis n'importe quel point d'entrée								
	Renforcer les mécanismes d'authentification sur les applications et/ou sur les postes de travail								
	Maîtriser l'ouverture de son SI et l'externalisation de services								
	Disposer d'un annuaire central pour gérer les identités et les accès								
	Maîtriser et tracer l'allocation, la modification et le retrait des droits des utilisateurs sur le SI								
	Supprimer les comptes orphelins, s'assurer du non-cumul de droits toxiques								
	S'assurer de la clôture effective des comptes pour les personnes ayant quitté l'entreprise								
Ergonomie & satisfaction utilisateurs	Disposer d'une authentification unique et ergonomique pour toutes les applications								
	Rendre les utilisateurs autonomes sur la réinitialisation de leurs mots de passe								
	Déléguer l'authentification à des fournisseurs d'identités tiers								
	Uniformiser les parcours utilisateurs quel que soit le support utilisé : interne, mobile, distant, etc.								
	Offrir un portail self-service de demandes d'accès à des applications du SI								
	Simplifier les processus d'affectation et de retraits de droits								
	Simplifier les tâches opérationnelles de revues								
Coûts / ROI	Alléger la gestion des mots de passe et leur renouvellement								
	Standardiser et mutualiser les infrastructures d'authentification et d'autorisation								
	Simplifier l'intégration et le raccordement des nouveaux services dans le SI								
	Réduire les tâches administratives								
	Améliorer l'efficacité et la fiabilité des processus d'entrée, mobilité, sortie et d'allocation de droits								
	Automatiser le provisionnement des comptes et des droits dans les applications du SI								
	Supprimer les processus utilisant des formulaires « papier »								

Domaines	Exemples de problématiques et de cas d'usages	Auth. forte	SSO	Fédération	Annuaire	Cycle de vie	Habilitations	Revues	Rôles
Urbanisation, Standards	Définir un socle d'authentification indépendant des implémentations spécifiques								
	Simplifier l'intégration de nouvelles applications et apporter de la flexibilité et de l'agilité dans le SI								
	Disposer d'un référentiel central, unique et fiable des identités et des droits								
	Homogénéiser les politiques de sécurité globales au SI								
Business	Accompagner les mouvements de fond d'ouverture de son SI vers des tiers ou vers le Cloud								
	Faciliter les accès aux applications dans des contextes de transformation de l'entreprise								
Conformité	Répondre aux exigences réglementaires nécessitant la mise en œuvre d'une authentification forte								
	Répondre aux contraintes du contrôle interne, des régulateurs, des commissaires aux comptes								
	Faciliter les revues d'habilitations et la réalisation d'audit et de contrôles								
	Permettre le contrôle du respect du principe de la SoD								

0

IV. Avant de démarrer : idées reçues, pièges à éviter, …

Un projet IAM/IAG ne se limite pas au déploiement d'un produit technique installé dans une logique « plug&play ». C'est un projet plus emblématique, plus fonctionnel, plus organisationnel, dont la mise en œuvre peut échouer par manque de vigilance sur tout un ensemble de points.

L'objet de ce chapitre est ainsi de lister quelques sujets qui correspondent soit à des idées reçues qu'il faut évacuer rapidement, soit à des pièges facilement évitables, soit tout simplement à des conseils pratiques.

La suite du document reviendra sur chacune des phases du projet, de manière plus détaillée. La section « prérequis » des « fiches pratiques » fournit des éléments plus précis par rapport à un contexte donné.

IV.1. Quelques idées reçues…

« L'IAM est magique »

Malheureusement, l'IAM n'a rien de magique. Il ne va pas traiter d'un coup de baguette un flou organisationnel, l'absence d'homogénéité dans la définition des profils métiers ou encore une obsolescence technique rendant les applications incompatibles avec les standards actuels.

Ainsi, pour limiter les déceptions, il est nécessaire :

- d'évaluer sa « maturité IAM » ;
- de construire une roadmap qui permette d'augmenter cette maturité ;
- de préciser les prérequis nécessaires à chaque étape pour tirer pleinement parti de l'IAM.

Par exemple, un projet IAM ne va pas intégrer l'ensemble des applications du SI dans son périmètre, tout du moins lors des premières phases du projet, notamment sur le volet « provisioning des comptes et des droits ».

Attention donc aux déceptions de type « l'IAM s'arrête aux portes du SI ». Il faut être réaliste, bien communiquer sur le périmètre de son projet, voire sur un premier périmètre, pour ne pas susciter ces déceptions. Il faut également savoir s'adapter si besoin aux technologies du marché, aux processus internes, au budget, etc.

« Gérer le projet tout seul pour aller plus vite et avoir moins d'ennuis »

La mise en œuvre de ce type de projet impacte très souvent l'organisation dans son ensemble. L'IAM est un projet transverse qui peut perturber l'organisation. Il est par conséquent essentiel de communiquer et d'impliquer toutes les parties prenantes. Cela va des métiers, aux RH, en passant par la direction générale, la DSI, les contrôleurs, les auditeurs, etc. La meilleure approche est évidemment de s'en faire des alliés, en trouvant les arguments qui les touchent et en sollicitant dès le début les acteurs ayant un enjeu avec la cible. (cf. fiches pratiques plus loin dans le document).

IV.2. Quelques pièges à éviter …

« Faire l'acquisition d'un progiciel avant même d'avoir défini son besoin »

C'est bien là une des premières erreurs à ne pas commettre. Si les progiciels d'IAM font ce pourquoi ils ont été écrits, ils ne le font pas tous de la même façon, et ils n'ont pas forcément tous la même couverture fonctionnelle.

De même qu'il ne faut pas « mettre la charrue avant les bœufs », il ne faut pas se jeter sur telle ou telle solution au titre d'un choix groupe par exemple, d'une période de solde sur les prix ou d'un conseil un peu trop subjectif, avant même d'avoir une bonne vision de ce qui est attendu à court, moyen et plus long termes en matière d'IAM.

Il est facile de comprendre par exemple qu'une petite filiale d'un grand groupe ne peut pas forcément utiliser et déployer les solutions du groupe, non adaptées fonctionnellement et techniquement. Si le SI est d'une taille raisonnable, il peut être préférable d'envisager des procédures manuelles pour commencer et répondre aux besoins prioritaires du projet.

A contrario, une fois la solution choisie, la logique doit s'inverser. Il est indispensable de creuser dans le détail le fonctionnement de la solution, en s'appuyant éventuellement sur un partenaire, pour rester dans l'épure de la solution et ainsi limiter les développements spécifiques. De plus, des fonctionnalités non imaginées au départ peuvent être disponibles et simplifier la couverture de certains cas d'usages.

« Vouloir tout faire d'un coup »

Attention au périmètre de départ. Il ne faut pas s'imaginer mettre en œuvre en une seule fois son projet d'IAM. L'approche itérative est de loin la meilleure : par modules fonctionnels, par entités géographiques ou organisationnelles, par périmètre d'utilisateurs ou d'applications, etc.

Il faut ainsi avancer pas à pas, en commençant avec un périmètre réduit et maîtrisé pour comprendre la mécanique des progiciels mis en œuvre. La logique de « Big Bang » a définitivement laissé la place à une approche par lots. Là aussi, il faut l'annoncer aux parties prenantes, afin d'éviter les déceptions.

« Raisonner à court terme »

L'IAM ne s'arrête jamais. Une fois le projet mis en œuvre, il continue. Il s'agit d'un système très dynamique, qui vit longtemps après le « build » initial. Il est fondamental de savoir qui va gérer le projet une fois cette première phase terminée, qui va l'exploiter, qui va le faire évoluer, etc. Il faut ainsi disposer d'une garantie de continuité de service ; sinon mieux vaut ne pas démarrer.

« Penser savoir comment les gens travaillent au quotidien »

Vous connaissez l'organisation de votre entreprise, ses principales filières métiers, ses cas particuliers majeurs, ses évolutions passées et peut-être ses évolutions futures probables.

Mais connaissez-vous suffisamment les modalités opérationnelles et les contraintes de travail de chacun ? Celles des employés sédentaires et des employés en déplacement ? Avec ou sans bureau ? Avec un accès réseau de faible débit, loin des équipes support ou en horaires décalés ? Quid des organisations en période de vacances ? Etc.

Un projet IAM sera nécessairement confronté à la réalité opérationnelle du terrain, et ne pourra être apprécié que s'il simplifie les usages au quotidien en tenant compte des spécificités légitimes. Il est donc nécessaire d'aller au-delà des principes d'organisation pour :

- comprendre opérationnellement comment fonctionne l'entreprise ;
- confronter ces usages au modèle organisationnel théorique ;
- séparer les « biais opérationnels » qu'il ne faut pas prendre en compte dans l'IAM, des « spécificités réelles » auxquelles l'IAM doit s'adapter.

IV.3. Quelques conseils avant de commencer…

« Connaître son SI »

Le SI est très souvent marqué par un historique, avec une hétérogénéité des systèmes, ce qui renforce la complexité de l'implémentation d'un projet IAM. Afin de limiter au maximum les mauvaises surprises, il est très fortement conseillé d'identifier clairement, et le plus tôt possible, les responsables fonctionnels et techniques du parc applicatif pour les impliquer très en amont dans la phase d'étude préalable.

« Bien définir son besoin »

Il est indispensable de bien cadrer ses besoins à court terme, ainsi qu'à moyen et long termes s'ils sont connus. Cela permet de tracer sa feuille de route et de définir les étapes de son projet. La tentation de rajouter du fonctionnel en permanence est grande mais il ne faut pas y céder, au risque de ne jamais démarrer le projet. Mieux vaut lotir, itérer et prévoir des évolutions, dans la mesure du possible, tout en considérant la cohérence du périmètre utilisateur.

« Ne pas mélanger les genres »

A trop vouloir simplifier, certains raccourcis peuvent s'avérer erronés.

Par exemple, la gestion du cycle de vie des utilisateurs internes au SI ne peut pas être traitée de la même façon que celle des clients externes. Les contraintes, les volumétries sont différentes. Il est ainsi possible d'avoir un millier de collaborateurs internes mais des millions d'identités de clients à gérer, les processus sont alors différents. Cette logique s'applique également aux applications à gérer dans un projet de SSO ou de fédération d'identités, dans un projet d'authentification forte, etc.

Sortir des dénominations « IAM », « IAG », « IAI » ambiguës

Parler d'« IAM », « IAG », « IGA », « IRM », « IAI », « IDaaS », etc. peut être une source majeure de confusion, y compris pour les fournisseurs. C'est d'autant plus vrai que chaque étape du projet pourrait ne couvrir qu'une partie limitée de ces notions.

A titre d'illustration :

- des fonctionnalités de recertification d'identités pourront grandement améliorer la qualité des données dans une étape centrée sur la gestion des identités et la création d'un référentiel d'identité ;
- une étape de recertification de droits peut grandement aider à la définition de profils métiers et à l'évolution du modèle d'habilitation.

« Maîtriser le vocabulaire »

Le vocabulaire utilisé semble facile et compréhensible par tous, mais il ne faut pas se méprendre. Au sein d'une même organisation, tout le monde sait-il faire la différence entre une habilitation ou une autorisation ? Une authentification ou une identification ? Quelle est la définition d'un compte, d'un rôle, d'un profil ?

Il est essentiel de bien maîtriser la terminologie de ce type de projet afin d'éviter les contre-sens. La réalisation d'une présentation et d'un glossaire interne, illustrés d'exemples parlants, est très souvent une bonne approche pour que tout le monde utilise le même langage.

« Maîtriser sa communication »

Maîtriser sa communication, c'est avant tout identifier les impacts du déploiement de son projet et ainsi pouvoir anticiper, cibler et contrôler sa communication. Il s'agit de discerner les acteurs concernés, quand et comment les impliquer, comment valoriser les gains, etc.

V. Avant – projet : les questions à se poser…

L'objet de ce chapitre, construit selon un modèle de « FAQ », est de fournir quelques recommandations et conseils importants à prendre en considération dans la phase d'avant-projet. Ceux-ci concernent notamment le travail préparatoire nécessaire à mettre en œuvre, le contenu de son cahier des charges, le choix des solutions.

Les questions traitées ci-après sont les suivantes :

Q1 : Dois-je me faire accompagner avant de lancer mon projet ?

Q2 : Quel lien entre les équipes fonctionnelles et les équipes techniques ?

Q3 : Faut-il analyser au préalable les solutions IAM du marché ? Lesquelles ? Combien ? Et comment prendre en compte les rapports des analystes ?

Q4 : Que dois-je préparer en amont de mon projet ?

Q5 : De quelle organisation ai-je besoin avant de démarrer mon projet ?

Q6 : Quelles sont les contraintes juridiques à prendre en compte ?

Q7 : Faut-il impliquer les achats dès le début du projet ?

Q8 : Quels sont les éléments à ne pas oublier dans mon cahier des charges ?

Q9 : A qui dois-je envoyer mon dossier de consultation ?

Q1	**Dois-je me faire accompagner avant de lancer mon projet ?**

Une autre manière de poser cette question pourrait être « Ai-je l'expertise et l'expérience en interne pour mener mon projet ? ».

Il existe de nombreux experts du domaine de l'IAM sur le marché de la sécurité. Aussi il peut être intéressant de s'appuyer sur eux, sachant que leurs prestations peuvent prendre différentes formes, à différents coûts.

Évidemment, le volume de jours d'accompagnement est fonction de la mission, de la taille de l'entreprise, du périmètre du futur projet, de l'organisation en place dans l'entreprise, mais aussi de la capacité à engager de telles prestations. Par exemple :

- Pour des prestations à coût faible de quelques dizaines de jours/hommes : cadrage initial, sensibilisation, analyse macroscopique afin de « mettre le projet sur les rails », évaluation du budget - élément fondamental pour savoir si l'entreprise a les moyens de ses ambitions - et définition de la feuille de route.
- Pour des prestations plus lourdes :
  - assistance à la rédaction de l'expression de besoins, du cahier des charges, au dépouillement, à la mise en place et au suivi du PoC ;
  - assistance à la description détaillée des processus d'entrée/mobilité/sortie, à la cartographie des applications, à la définition des rôles et profils de l'organisation, etc.

Toutefois, un prestataire ne saurait mener le projet seul. Il devra s'appuyer sur une équipe interne, légitime dans l'organisation. En effet, un prestataire pourra amener son éclairage mais ne saurait se suppléer au client pour décider des priorités à retenir ou réaliser les arbitrages nécessaires.

Il est donc très important de définir ce qui est attendu du prestataire et ce à quoi s'engage le client, ce qui ne dispense pas d'acquérir une expertise minimale avant de démarrer, la lecture de ce guide étant un bon début.

Q2	**Quel lien entre les équipes fonctionnelles et les équipes techniques ?**

Les projets IAM/IAG sont à la fois fonctionnels, organisationnels et techniques. La question du lien entre les équipes fonctionnelles et les équipes techniques est donc naturelle. Pour les entreprises s'appuyant sur une séparation AMOA et MOE, il est indispensable que les équipes travaillent en forte proximité, se comprennent et se fassent confiance pour réaliser, ensemble, les meilleurs arbitrages. En effet, il est toujours préférable de tirer parti des fonctionnalités natives offertes par les solutions à mettre en place, quitte à légèrement adapter la manière de couvrir les besoins exprimés.

Par exemple, plutôt que d'implémenter des contrôles et des workflows de demandes très complexes, il peut être préférable de maintenir un minimum de contrôles simples lors de la demande et de traiter les cas plus avancés avec des contrôles a posteriori. Cela permet d'offrir des processus de demande réactifs, d'utiliser des fonctionnalités natives tout en maintenant le niveau de sécurité souhaité. Cela s'applique par exemple pour les mobilités internes, avec période de biseau. Dans ce cas, une revue des anciens droits un mois après la mobilité est simple à implémenter, conforme à la « réalité du terrain » et souvent suffisante en matière de sécurité.

Idéalement, si un mariage AMOA-MOE est possible, pouvoir s'appuyer sur un partenaire unique est une solution idéale, et *a minima* une solution à étudier.

Q3	**Faut-il analyser au préalable les solutions IAM du marché ?** **Comment prendre en compte les rapports des analystes ?**

Toutes les solutions IAM ne répondent évidemment pas à tous les besoins, ou pas de la même manière. Ainsi il est souvent conseillé de prendre le temps d'en analyser au préalable quelques-unes.

De plus, si l'analyse de solutions du marché a notamment l'avantage d'aider au cadrage des besoins et à l'estimation de son budget, elle peut faire apparaître d'autres besoins ou mettre en évidence des points durs ou des éléments qui auraient été négligés.

Plusieurs méthodes d'analyse sont possibles :

- Lorsqu'un accompagnement est choisi, cf. question précédente Q1, un « état de l'art » des solutions au regard de ses besoins peut faire partie de la prestation d'accompagnement. Il faut dans ce cas s'assurer de l'impartialité du prestataire qui doit évidemment avoir des compétences d'intégration d'un certain nombre de solutions pour pouvoir en donner les avantages et inconvénients en fonction du contexte de son client.
- Sans pour autant se faire accompagner, il est aussi possible de se renseigner en participant à divers évènements : salons spécialisés, qui rassemblent en général une bonne partie des acteurs du marché de l'IAM/IAG, conférences, groupes de travail, etc. Ce type de pratiques permet en général de se bâtir une « culture IAM », facilitant le fait d'avoir *a minima* un avis sur la question.
- Les grands cabinets d'analystes (*Gartner, Forrester, KuppingerCole,* etc.) fournissent également un certain nombre d'outils et de rapports sur les solutions du marché. Attention à les considérer comme des influences et à ne pas les suivre aveuglément car les critères d'évaluation et de classements utilisés dans les rapports d'analystes ne sont pas forcément les mêmes pour tout le monde.
- La visite de clients références d'éditeurs sélectionnés est également un très bon moyen de s'assurer de la qualité des implémentations, de façon très concrète.
- Enfin, la meilleure approche, lorsqu'il est possible de la mettre en œuvre car elle demande plus de travail que les autres, reste souvent celle du PoC. Ce dernier doit se faire sur un périmètre réduit mais représentatif des besoins à court et moyen termes. Attention à ne pas évaluer trop de solutions, trois maximum en général, afin de ne pas y passer trop de temps, en s'appuyant sur une des méthodes ci-dessus pour établir une première liste de solutions favorites à évaluer.

Il est également conseillé d'avoir une vision « long terme » dans l'investissement. Un premier projet « court terme », par exemple un module de self-service de réinitialisation de mots de passe, peut s'inscrire dans un projet plus vaste à plus long terme, par exemple d'enterprise SSO, de WebSSO ou de fédération d'identités. Cette phase d'analyse préalable permet de s'assurer – au moins sur le papier - que la solution choisie répondra également aux besoins « long terme ».

Enfin, certains pourront aussi faire le choix de ne rien regarder ou évaluer avant de sortir leur appel d'offres, afin de ne pas avoir d'influences diverses. Cette pratique introduit un risque important, à savoir celui d'exprimer des exigences pour lesquelles aucune solution du marché ne répondra, et d'être ainsi décalé par rapport au marché.

Q4	Que dois-je préparer en amont de mon projet ?

Cela dépend directement de la nature du projet, les prérequis n'étant pas les mêmes pour un projet de fédération d'identités ou un projet de gouvernance des habilitations par exemple.

Cependant, et de manière générale, il est indispensable de mesurer son niveau de maturité IAM par rapport à la cible visée. En d'autres termes : ai-je les moyens, à savoir la légitimité, l'organisation, les processus, la technicité, le budget, le planning, etc. de mes ambitions ?

Les « fiches projet » du chapitre suivant (sections 3 et 4 de chaque fiche en particulier) apportent une réponse plus détaillée à cette question.

Q5	De quelle organisation ai-je besoin avant de démarrer mon projet ?

La réponse est similaire à celle de la question Q4, cela dépend des briques IAM/IAG souhaitées. Les « fiches projet » traitent ainsi le sujet, par brique, pour savoir :

- Qui finance le projet ?
- Qui pilote le projet ?
- Qui est responsable de la recette et de l'acceptation de la solution ?
- Qui aura la responsabilité de la plateforme une fois qu'elle aura été mise en œuvre ?
- Etc.

Q6	Quelles sont les contraintes juridiques à prendre en compte ?

Elles dépendent de différents paramètres, tels que la nature du projet IAM/IAG mené et le secteur d'activité de l'entreprise.

Par exemple, pour un projet d'authentification forte à base de certificats électroniques, il faudra utiliser des certificats RGS dans l'administration et des cartes CPS / CPE dans le secteur de la Santé. Il faudra également, dès lors qu'un référentiel d'identités est mis en place, s'assurer des obligations de protection des données à caractère personnel encadrées par la CNIL et par les nouveaux règlements européens eIDAS et GDPR. Les domaines de la finance et de l'assurance ne sont pas en reste avec les nombreuses normes et règlementations qui peuvent avoir un impact sur le projet, telles que SOX, PCI DSS, etc.

Dans certains contextes, les obligations légales peuvent être assez simples et se limiter à quelques précisions dans la charte informatique ou dans la PSSI. Dans d'autres, elles peuvent être plus contraignantes avec, par exemple, la rétention de logs, la conservation des informations d'habilitation, les contrats fournisseurs, etc.

Dans tous les cas, il est nécessaire d'impliquer son service juridique afin de connaître dès le début du projet les contraintes juridiques à prendre en compte.

Q7	**Faut-il impliquer les achats dès le début du projet ?**

Dans certaines organisations, les achats doivent être sollicités assez tôt. Dans ce cas, la question ne se pose plus. Dans les autres cas, il est surtout important de connaître quelles sont les contraintes liées aux achats afin de les anticiper : par exemple sur le chiffre d'affaire minimum ou le référencement des éditeurs de solutions ou des intégrateurs portant l'engagement de résultat.

Q8	**Quels sont les éléments à ne pas oublier dans mon cahier des charges ?**

De manière générale, tout ce qui pourra permettre de gagner du temps lors du cadrage et du démarrage du projet est bon à prendre. De même, plus la description des objectifs et des exigences sera précise, plus la comparaison des aspects techniques et financiers des différentes propositions reçues sera facilitée.

Quelques conseils simples :

- fournir tous les éléments qui permettront de ne pas avoir à comparer des offres trop différentes. Par exemple :
  - un périmètre précis sur lequel les soumissionnaires doivent s'engager : utilisateurs, applications, processus, exigences, contraintes, etc. :
    - Gestion d'identités : quelles populations sont adressées ? suivant quels processus ? sur quels périmètres ?
    - SSO : quelles sont les caractéristiques des applications ? quels sont les cas d'usages ? accès interne / externe, type de poste, types d'utilisateurs ?
    - Provisioning : quels objets ? quelles cibles ? quelles sources ? nature, technologies sous-jacentes, versions, contenus, comptes/profils/droits, cas d'usages ?
    - Gouvernance des habilitations : existant et états des lieux relatifs aux rôles/profils identifiés dans l'organisation ? gestion de rôles ? quelle granularité des droits gérer ? pour quelles cibles ?
  - la quantité et le niveau de livrables attendus ; cela aura un impact sur la gestion de projet proposée ;
- éviter toutes les questions ou exigences inutiles, qui viennent plus « polluer » la clarté des réponses des éditeurs et/ou intégrateurs, ou complexifier l'analyse des dossiers qu'autre chose. Ce n'est pas le volume ou le nombre de pages du cahier des charges qui compte, mais bien son niveau de précision et la clarté des informations fournies et des exigences exprimées. Par exemple, ne pas demander un support H24/7 à couverture internationale si ce n'est pas nécessaire ;
- dans le même esprit, éviter l'effet « liste au Père Noël » en laissant les soumissionnaires trop libres de proposer ce qu'ils veulent. Le risque est encore une fois d'avoir à analyser des propositions commerciales et techniques très différentes et d'avoir notamment des écarts de prix conséquents. Si cette approche est choisie, donner dans ce cas des priorités sur les éléments les plus importants, et proposer un cadre de réponse précis et relativement « fermé » ;
- indiquer quels sont les critères d'évaluation et de choix les plus importants, sans nécessairement fournir la totalité de sa grille de notation au risque d'influencer les réponses, communiquer *a minima* une pondération de ces critères.

Quelques pièges à éviter lors de la rédaction de son cahier des charges :

- confondre capacité des solutions techniques et périmètre de la prestation : les solutions techniques offrent un large panel de fonctionnalités et il est donc primordial de définir ses priorités et le contexte dans lequel la solution doit être mise en œuvre ;
- demander toutes les fonctionnalités en production en moins de 6 mois. Les projets IAM étant souvent très attendus, une certaine pression temporelle est souvent appliquée. Ayez à l'esprit que tout projet IAM, quel qu'il soit, nécessite en amont une définition de l'organisation, des cas d'usages et des processus. Il est illusoire de mettre en production une solution technique sans avoir passé du temps sur la phase préparatoire ;
- ne pas détailler son existant. Plus les soumissionnaires auront d'informations sur l'existant, plus les réponses seront précises et homogènes. Certaines fonctionnalités ou applications étant très structurantes dans ce type de projet, chaque oubli ou imprécision amènera inévitablement à des incompréhensions et donc à des difficultés de mise en œuvre par la suite.

L'annexe 2 fournit une possible structure « type » d'un cahier des charges IAM/IAG.

Q9	**A qui dois-je envoyer mon dossier de consultation ?**

Il y a plusieurs écoles, l'engagement pouvant être demandé à l'éditeur, à l'intégrateur, aux deux. Dans les faits, plusieurs approches sont pratiquées :

- émission d'un appel d'offres orienté « Solution intégrée » : dans ce cas une solution complète sera demandée, englobant une ou plusieurs solutions, intégrées par un ou plusieurs intégrateurs avec un point d'entrée unique ;
- choix de solution en phase 1, puis choix d'un intégrateur en phase 2 pour intégrer la solution, selon le souhait de l'intégrer en interne après formation ;
- choix d'un intégrateur en phase 1, puis choix d'une solution en phase 2 selon ses analyses, conseils et compétences

Chaque approche a ses avantages et inconvénients, et dépend évidemment de la maturité et de l'expertise de l'entreprise en la matière, des processus internes à l'organisation. De même que pour les points précédents, il est possible de fournir quelques conseils simples :

- bien préciser à qui va être demandé l'engagement relatif à l'intégration de son projet ;
- ne pas envoyer son cahier des charges à tout le marché des éditeurs et intégrateurs, au risque d'avoir énormément de travail de dépouillement et de sélection des offres ; exception faite pour le secteur public qui exige un appel d'offres ouvert ;
- s'adresser à des spécialistes, capables d'afficher des expériences positives dans le domaine de l'IAM/IAG. Lorsque le choix est fait de travailler avec un intégrateur généraliste, par exemple pour des questions de référencement achat, il est nécessaire de s'assurer qu'il embarque obligatoirement en sous-traitance de l'expertise de l'éditeur de la solution proposée, ou d'un intégrateur spécialiste sur cette solution, et exiger d'avoir un accès direct à l'expert et ce sans intermédiaire en cas de difficultés ;
- faire la démarche de rencontrer des acteurs du marché, intégrateurs et éditeurs, en amont de la consultation pour se faire sa propre idée sur leurs compétences et mode de fonctionnement ;

- raisonner à « long terme » : le ou les produits qui seront installés dans le cadre du projet le seront pour plusieurs années. Il faut bien identifier qui assurera les supports niveaux 1 et 2, sachant que le support niveau 3 est forcément apporté par le développeur du produit, donc l'éditeur.

Par ailleurs, voici quelques notions importantes à garder en mémoire :

- l'intégrateur spécialiste et expert sur toutes les solutions du marché n'existe pas. De même, rares sont les éditeurs proposant l'exhaustivité des briques logicielles qui composent le monde de l'IAM/IAG ;
- les éditeurs n'ont pas forcément des services professionnels locaux et un support local, qui plus est dans toutes les langues. Ce point peut être gênant dans certains cas ;
- la valeur ajoutée de l'intégrateur augmente avec le nombre de solutions à mettre en place dans le cadre du projet : il est le point d'entrée unique ayant les compétences sur toutes les briques à mettre en œuvre, éventuellement issues d'éditeurs différents.

VI. Mise en œuvre d'un projet IAM - Fiches pratiques

VI.1. Introduction

Dans cette section, nous proposons un certain nombre de fiches pratiques, à la manière de « recettes de cuisine », en proposant un découpage par module fonctionnel de l'IAM/IAG. Ces fiches peuvent évidemment être combinées.

L'objectif est de lister un maximum de points clés, en répondant, pour chaque module fonctionnel, aux questions suivantes :

- Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?
- Comment vendre le projet en interne ?
- Quels sont les éléments spécifiques à prendre en compte dans le budget du projet ?
- Quelles sont les étapes clés du déploiement ? les questions à se poser et les points à ne pas négliger ?
- Quels sont les points clés pour réussir la mise en place d'un tel projet ?

Nous avons également souhaité produire un document « digeste ». Par conséquent nous nous sommes concentrés essentiellement sur les éléments les plus spécifiques de chacun des modules présentés dans le cadre d'une démarche projet classique.

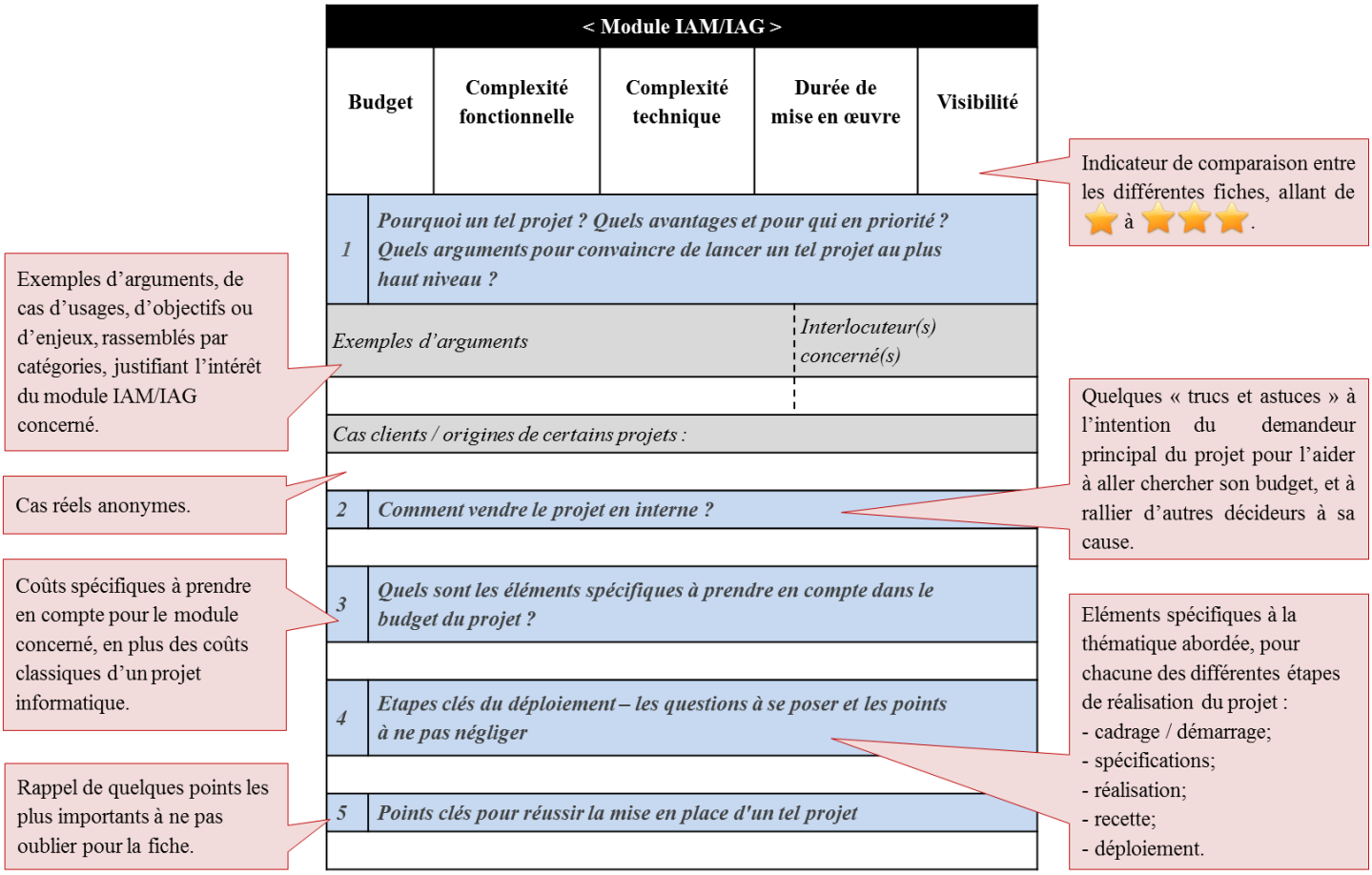
Enfin, comme précisé en début de document, nous n'avons volontairement pas abordé l'ensemble des briques fonctionnelles de l'IAM/IAG, et nous nous sommes limités aux modules suivants :

Les fiches suivantes sont présentées ci-après :

- Fiches « Accès »
  - **SSO – Single Sign-On**, qui regroupe les modules eSSO et WAM
  - **Fédération des identités**
  - **Authentification forte**
- Fiches « Identités »
  - **Annuaire d'identités**
  - **Cycle de vie des utilisateurs**
  - **Gestion des habilitations**
- Fiches « Gouvernance »
  - **Revue des habilitations / Recertification**
  - **Gestion de rôles**

VI.1.1. How to ? Guide de lecture des fiches pratiques

Les fiches pratiques se présentent toutes sous la forme ci-dessous :



Les étoiles attribuées aux cinq critères situés dans la partie supérieure de la fiche sont des indicateurs de comparaison de niveau allant de un à trois. Les notes ci-dessous ont été positionnées collégialement par les membres du GT IAM sur la base de leur expérience.

L'idée est ainsi :

- de positionner les différents modules de l'IAM /IAG les uns par rapport aux autres ;
- de visualiser simplement les caractéristiques majeures de chaque fiche.

Les prérequis sont considérés comme acquis dans cette analyse, et le lecteur est invité à confronter son contexte organisationnel et technique pour ajuster l'échelle.

Enfin les exemples de cas clients présentés sont réels et rendus anonymes pour des questions de confidentialité.

VI.1.2. Vue générale

Le tableau ci-dessous synthétise les « notes » de chaque fiche pratique détaillée dans les paragraphes suivants.

	Budget	Complexité fonctionnelle	Complexité technique	Durée de mise en œuvre	Visibilité
SSO Single Sign-On	★	★	★	★	★★★
Fédération d'Identités	★	★	★	★	★★★
Authentification forte	★★★	★	★	★	★★★
Annuaire d'identités	★★	★★	★	★	★★★
Cycle de vie des utilisateurs	★★	★★	★★	★★	★★
Gestion des habilitations	★★★	★★★	★★	★★	★★
Revues d'habilitations	★★	★★	★	★★	★
Gestion des rôles	★★★	★★★	★★	★★★	★★

VI.2. Access Management / Gestion des Accès

VI.2.1. Fiche « SSO – Single Sign-On »

<table>
<tr><th colspan="6">« SSO – Single Sign-On »</th></tr>
<tr><th>Budget</th><th>Complexité fonctionnelle</th><th>Complexité technique</th><th>Durée de mise en œuvre</th><th colspan="2">Visibilité</th></tr>
<tr><td>★</td><td>★</td><td>★</td><td>★</td><td colspan="2">★★★</td></tr>
<tr><td>1</td><td colspan="5">Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?</td></tr>
<tr><td colspan="4">Exemples d'arguments</td><td colspan="2">Interlocuteur(s) concerné(s)</td></tr>
<tr><td colspan="4">• Sécurité
• supprimer l'effet « post-it » des mots de passe connus de tous ou l'utilisation de mots de passe triviaux ;
• contrôler les accès aux applications depuis n'importe quel point d'entrée ;
• homogénéiser les politiques de sécurité globales du SI ;
• renforcer les stratégies de mots de passe sur les applications ;
• mettre en place des mécanismes de délégation de comptes ;
• tracer les accès aux applications : authentifications et autorisations ;
• auditer la sécurité et disposer de statistiques des accès au SI, y compris sur les postes ou les applications partagées entre plusieurs utilisateurs.</td><td colspan="2">RSSI</td></tr>
<tr><td colspan="4">• Ergonomie / Confort & satisfaction des utilisateurs
• simplifier la vie des utilisateurs en facilitant l'accès aux applications du SI ;
• disposer d'une authentification unique pour toutes les applications ;
• rendre les utilisateurs autonomes sur la réinitialisation de leurs mots de passe ou de leurs moyens d'authentification ;
• accéder à des services de type « portail SSO » ou « délégation de comptes » ;</td><td colspan="2">Utilisateurs</td></tr>
<tr><td colspan="4">• Coûts d'administration
• alléger la gestion des mots de passe et leur renouvellement ;
• standardiser et mutualiser les infrastructures d'authentification et d'autorisation ;
• simplifier l'intégration et le raccordement des nouveaux services dans le SI ;
• contrôler l'adéquation entre les licences payées et celles réellement utilisées, cas du Saas par exemple, via des rapports d'utilisation des applications.</td><td colspan="2">Direction Financière
Contrôle de gestion</td></tr>
</table>

Cas clients / origines de certains projets :

Cas client 1 : #Finance #Sécurité #150kUsers

- Déclencheur : Lutte contre la fraude.
- Objectifs principaux : Déléguer la fonction d'authentification pour plusieurs centaines d'applications Web internes et externes à un service dédié ; renforcer le contrôle d'accès ; mettre en place une authentification forte pour les applications « sensibles » ; généraliser le SSO pour les applications Web ; fournir un service de fédération d'identités SAMLv2 aux partenaires B2B.
- Solution : Déploiement d'une solution centrale de Web Access Management & fédération d'identités fournissant plusieurs méthodes d'authentification à 1, 2, ou 3 facteurs selon les cas ainsi que du SSO sur plusieurs centaines d'applications Web du groupe.

Cas client 2 : #GrandeDistribution #VendeursMobiles #Itinérance #Virtualisation #20kUsers

- Déclencheur : Passage de plus de cent-vingt SI, soit un par magasin, à un SI centralisé, avec mise en œuvre de virtualisation.
- Objectifs principaux : Diminuer les coûts du helpdesk, des mises à jour, etc. ; moderniser le système d'accès à l'outil informatique ; intégrer de nouveaux supports comme des tablettes ; faciliter la connexion via un périphérique d'accès ; garantir la sécurité et la confidentialité.
- Solution : Virtualisation des postes de travail sur des clients légers avec le déploiement d'une solution de eSSO apportant des fonctionnalités d'authentification forte via Badge RFID, connexion/reconnexion rapide, SSO dans les applications, et mobilité de la session.

Cas client 3 : #Service #Téléopérateurs #ResetPassword #ROI #20kUsers

- Déclencheur : Pertes régulières de mots de passe entraînant une baisse de productivité.
- Objectifs principaux : Les téléopérateurs travaillent sur une application différente par client du centre d'appel, chacune nécessitant une authentification dédiée via des couples login/mot de passe différents pour chaque application. Les oublis de mots de passe entraînent des blocages de comptes et l'impossibilité de se connecter en raison de tentatives répétitives erronées. L'objectif prioritaire est de diminuer les pertes de productivité en réduisant la fréquence des blocages de comptes et des périodes d'inactivité associées.
- Solution : Mise en place d'une solution eSSO garantissant un mot de passe unique, celui de l'ouverture de la session Windows, et une authentification transparente sur toutes les applications métiers.

2	***Comment vendre le projet en interne ?***

Avec l'aide d'un PoC

- La mise en place d'un PoC reste certainement la méthode la plus efficace pour vendre le projet en interne. Le PoC permet d'illustrer de façon concrète l'intégration d'une solution de SSO dans son SI et d'en mesurer les avantages attendus. Il permet également de s'impliquer, d'impliquer les métiers, et de cadrer le projet cible en amont.
- Si le PoC est convaincant, l'étape suivante est souvent celle du pilote. Elle consiste à étendre le périmètre du PoC à un périmètre plus large en termes d'utilisateurs - par exemple à tous ceux d'un service - ou d'applications en production.

- A noter qu'un PoC se prépare : il doit être réalisé dans un environnement représentatif de la cible visée : applications, postes de travail, usages, etc.

Par la mise en service de « Quick Wins »

- Les projets de SSO présentent l'avantage d'être mis en œuvre relativement rapidement, par exemple en quelques semaines selon le premier périmètre défini, et d'apporter du confort aux utilisateurs de l'entreprise via la mise à disposition d'une authentification unique.
- Exemples de « Quick Wins » visibles :
  - portail unique d'accès aux applications web : « Portail WebSSO » ;
  - self-service de réinitialisation de mots de passe ;
  - SSO en environnement mobile ;
  - authentification forte (cf. fiche dédiée) ;
  - fédération d'identités (cf. fiche dédiée).

3 Quels sont les éléments spécifiques à prendre en compte dans le budget du projet ?

Un projet de SSO peut engendrer des coûts spécifiques si le projet est lié à un projet d'authentification forte. Cf. fiche dédiée sur l'« authentification forte » ci-après.

De même, dans certains cas, l'intégration d'une application dans le projet de SSO peut nécessiter une modification de cette application : par exemple si elle doit être « SAML-Ready », raccordée à une solution de type CAS, ou implémenter une API de la solution de SSO choisie.

4 Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger

Pendant le cadrage / démarrage du projet

Comme souvent, il est fondamental de bien définir le périmètre organisationnel et fonctionnel du projet. Il est nécessaire d'avoir au préalable les réponses aux questions ci-dessous :

- Ai-je un référentiel d'identités pour appuyer mon service de SSO ? Sa qualité des données est-elle suffisante ?
- Quels seront les utilisateurs du SSO : tous, certaines structures seulement, le siège, les agences, certaines filiales ?
- Quelles applications seront prises en compte ? Quel « type » de SSO mettre en œuvre : Enterprise SSO ? Web Access Management ? Fédération d'identités ? Mobile SSO ? Tous ?
- Quels seront les acteurs impliqués dans le projet : RSSI, responsables/gestionnaires d'applications, exploitants, éditeurs, etc.?
- Existe-il déjà des moyens d'authentification à prendre en compte ? Y a-t-il des contraintes d'usage, de technologie, de législation ou autre à prendre en compte pour l'authentification ?
- Les applications concernées par le projet sont-elles maîtrisées ? Idem pour les postes de travail ?
- Les utilisateurs doivent-ils continuer à connaître leurs mots de passe ? Quel est le niveau de sécurité attendu du projet ?
- Quels sont les modes dégradés attendus, et les délais associés à ce type de situation ?

Pendant les spécifications fonctionnelles et techniques

Il est conseillé de travailler par « atelier thématique » :

- ateliers fonctionnels : cas d'usages utilisateurs, cinématiques d'authentification, d'accès aux applications, d'enrôlement, de délégation, de réinitialisation de mots de passe, cinématiques métier de bout en bout (connexion, accès applicatif, validation fonctionnelle, changement d'utilisateur, etc.) ;
- ateliers techniques : architecture globale, éléments structurants de l'architecture comme les pics de connexion, la montée en charge, les référentiels d'authentification, les types de postes, la localisation du matériel pour l'accès ;
- applications : travailler par « fiches de description d'application » - cf. exemples en annexes IX.3.

La mise en œuvre d'une maquette ou d'un PoC, si cela n'a pas été fait en phase amont du projet, permet de s'appuyer sur des éléments concrets dès la phase de conception.

Pendant la phase de réalisation

Ne pas négliger l'organisation de tests de montée en charge si ce critère est important pour le projet à venir.

Pendant la phase de recette

Il est conseillé de tester les modes et procédures de connexion dégradés/alternatifs. Le risque qu'ils ne fonctionnent pas lorsqu'ils sont nécessaires est réel s'ils n'ont pas été testés en recette.

Pendant la phase de déploiement

Une démarche efficace est souvent de commencer par un périmètre pilote, puis de généraliser le déploiement par itération, lot après lot, chaque lot pouvant porter :

- dans le cas d'un projet « eSSO », sur un nouveau périmètre d'utilisateurs ou de postes de travail, par exemple par service, site, agence ou filiale ;
- dans le cas d'un projet « WebSSO », sur de nouvelles applications attachées au projet ;

Les étapes de transfert de compétence et de prise en main par les équipes responsables du déploiement et de l'exploitation sont également réalisées pendant cette phase.

5 Points clés pour réussir la mise en place d'un tel projet

Quelques points clés :

- bien cadrer son projet et maîtriser ses souhaits : l'expression des besoins et des objectifs du projet doit être claire. Le besoin doit être défini avant le choix de la solution, et non l'inverse ;
- s'assurer de disposer d'un référentiel des identités de qualité, des moyens de contrôler la qualité de ces données et de la légitimité pour demander des éventuelles mises en qualité/ corrections de données ;
- choisir une solution adaptée à ses besoins : il est indispensable d'avoir une vision à « court terme » et à « long terme » afin de ne pas avoir à investir dans une autre solution un ou deux ans plus tard ;
- être proactif : tout ce qui est anticipé et préparé en amont du projet ne sera pas à refaire, par exemple l'analyse des applications et l'identification des responsables associés ;

- prévoir tous les modes dégradés possibles : par exemple en cas de perte ou oubli du mot de passe principal, du token d'authentification ou d'indisponibilité du système SSO, sachant que, dans ce dernier cas, un système SSO généralisé à la quasi-totalité des applications d'un grand groupe impose une architecture très haute disponibilité ;
- lotir le projet : commencer par un socle de base cohérent pour l'utilisateur avec un nombre limité d'applications qui y sont raccordées : applications les plus sensibles, les plus critiques ou les plus utilisées par exemple. Généraliser ensuite le déploiement par « packs » d'applications ou d'utilisateurs ;
- définir une stratégie et une méthodologie d'intégration d'applications existantes et futures dans le projet SSO ;
- ne pas négliger la conduite du changement et les coûts internes du projet.

VI.2.2. Fiche « Fédération des identités »

La fédération d'identités peut être considérée principalement sous deux angles :

- Sous un angle « business » : elle facilite les échanges B2B ou B2C et permet de s'affranchir d'un certain nombre de contraintes liées aux identités et aux mécanismes d'authentification en particulier.
- Sous un angle « technique » : elle s'impose de plus en plus comme un outil de mise en œuvre d'« architectures WebSSO », via l'utilisation de protocoles standards et normalisés tels que SAML, OAuth ou OpenIDConnect. Ceci notamment pour les applications disponibles en modes SaaS et Cloud et de plus en plus pour les applications mobiles.

De fait, il est souvent utile de préciser sous quel angle est abordée la fédération d'identités, même si ces deux positionnements ne sont évidemment pas incompatibles.

A noter que, pour les cas où la fédération est uniquement considérée comme un moyen de faire du WebSSO avec des applications « *federation-compliant* » ou « *federation-ready* », il est possible de se référer à la fiche technique SSO présentée précédemment, ainsi qu'à l'annexe « *IX.3.3. Questions spécifiques au WebSSO et à la fédération d'identités* ».

« Fédération des identités »				
Budget	**Complexité fonctionnelle**	**Complexité technique**	**Durée de mise en œuvre**	**Visibilité**
				

1	***Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?***

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Business** • accompagner le mouvement de fond vers le cloud ; • accompagner l'ouverture de son SI vers des tiers : partenaires, clients, etc. ; • faciliter les accès aux applications dans des contextes de transformation de l'entreprise : réorganisation, joint-venture, fusion/acquisition, division, etc. ; • faciliter la gestion des accès aux services mutualisés au sein d'organisations complexes ou de cercles de partenaires.	Direction Générale DSI RSSI
• **Ergonomie, services aux utilisateurs** • faciliter et uniformiser les parcours d'inscription et d'authentification à des services proposés à des utilisateurs externes ; • déléguer l'authentification à des fournisseurs d'identités tiers : France Connect, Google, Facebook, etc. ; • simplifier l'accès à des applications externes : services SaaS ou Cloud, de type O365, GoogleApps, etc. ou à des services proposés par des partenaires B2B ; • uniformiser les parcours utilisateurs sur tous les supports, Web ou mobile.	Direction Générale Marketing Digital
• **Urbanisation, standardisation** • définir un socle d'authentification indépendant des implémentations spécifiques ; • simplifier l'intégration de nouvelles applications dans le SI ; • apporter de la flexibilité et de l'agilité dans le SI ; • bénéficier de standards de fédération garantissant la sécurité et la traçabilité des accès dans une relation de confiance entre partenaires.	DSI RSSI Urbanistes du SI Architectes
• **Sécurité** • éviter de dupliquer les annuaires dans les infrastructures SaaS ou de donner un accès depuis l'extérieur à ses annuaires d'identités ou d'authentification ; • ne pas avoir à gérer les « identités des autres » ; • maîtriser l'ouverture de son SI et l'externalisation de services.	RSSI

Cas clients / origines de certains projets :

Cas client 1 : #Media #B2B #B2C #8MUsers

- Déclencheur : refonte et industrialisation de la plateforme de contrôle d'accès de l'ensemble des sites internet du groupe.
- Objectifs principaux : Sécuriser et améliorer la gestion de l'authentification et de l'accès aux services ; uniformiser les parcours d'inscription et d'authentification sur les supports Web et mobile ; implémenter l'interfaçage avec les réseaux sociaux et permettre l'utilisation d'identités numériques tierces ; devenir un hub d'authentification avec des fournisseurs d'identités tiers ; faciliter l'intégration des parcours sur tous les portails fédérés et sur tous les équipements.
- Solution : Mise en place d'une plateforme centrale d'authentification et d'accès aux services du groupe, agissant comme un hub de fédération d'identités multi-protocoles, et permettant de jouer le rôle à la fois de fournisseur de services et de fournisseur d'identités vis-à-vis de partenaires commerciaux.

Cas client 2 : #Retail #Magasins #Cloud #3kUsers

- Déclencheur : Apporter du confort aux utilisateurs du SI tout en garantissant un bon niveau de sécurité et de disponibilité. Ceci avec des usages très différents selon que les utilisateurs sont au siège ou en magasin, en mobilité, ou pas.
- Objectifs principaux : Fournir un accès aux applications GoogleApps à partir d'une seule authentification variable selon que l'utilisateur est au siège sur poste dédié, partagé ou mobile, ou en magasin sur poste dédié ou partagé, voire en mobilité pour les vendeurs.
- Solution : Mise en place d'une solution de contrôle d'accès mettant en œuvre plusieurs moyens d'authentification selon les cas, tels que Kerberos, Certificat, login/mot de passe associé à de la fédération SAMLv2, afin d'atteindre le monde GoogleApps de façon sécurisée et ergonomique, quel que soit le point d'entrée.

Cas client 3 : #Bank #B2B #SAMLv2 #9kUsers

- Déclencheur : Ouvrir l'accès à des applications monétiques hébergées par le client « Banque1 » aux utilisateurs internes ainsi qu'aux utilisateurs externes de son sous-traitant « Banque2 ».
- Objectifs principaux : Ouvrir son SI à des partenaires en toute sécurité ; contrôler les accès externes ; simplifier les procédures d'authentification et industrialiser le raccordement de services à un socle de fédération d'identités.
- Solution : Mise en œuvre d'une solution de fédération d'identités SAMLv2, grâce à laquelle les utilisateurs et les clients de « Banque2 » accèdent aux applications monétiques hébergées chez « Banque1 ».

2	***Comment vendre le projet en interne ?***

De nombreux arguments peuvent convaincre de démarrer un projet de fédération d'identités : l'ergonomie et l'expérience utilisateur, la sécurité, l'urbanisation ou la simplification. Il est souvent assez simple d'identifier un « déclencheur » à mettre en avant pour justifier le démarrage du projet, au moins sur un premier périmètre de type « QuickWin ». Par exemple l'accès à des nouveaux services Cloud, un accord commercial avec un nouveau partenaire B2B, l'ouverture d'un service pour des utilisateurs externes, le renouvellement ou le remplacement d'une solution WAM existante incompatible avec les derniers standards, etc.

3	***Quels sont les éléments spécifiques à prendre en compte dans le budget du projet ?***

Dans un projet de fédération d'identités « business », l'élaboration du « contrat de fédération » sur le plan juridique entre les différentes entités partenaires est un centre de coût. Il fait en effet appel *a minima* à des juristes des différentes parties dans un contexte B2B. Dans un contexte B2C les déclarations relatives à la protection des données à caractère personnel sont également à prendre en compte.

Dans un projet de fédération d'identités « technique », il est possible de devoir modifier certaines applications afin de les rendre compatibles avec les protocoles techniques de fédération souhaités. L'intégration de standards tels que SAMLv2, OAUth2 ou OpenID Connect peut en effet nécessiter des développements spécifiques, voire l'acquisition ou le développement de « kits » de fédération, qu'il faudra maintenir par la suite. Ceci éventuellement pour différents langages et frameworks de développement comme Java, .Net, ou Spring par exemple. Il faudra donc s'assurer de disposer du bon niveau de compétences pour ne pas avoir de mauvaises surprises par la suite.
Enfin, afin d'éviter d'avoir à réexpliquer à chaque fois comment raccorder telle ou telle application à son futur socle de fédération, il faudra sensibiliser les équipes de développement internes sur la fédération et l'application des bonnes pratiques de développement associées.

4	***Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger***

Pendant le cadrage / démarrage

Selon la nature et le type de fédération d'identités à mettre en place, il faudra anticiper les aspects juridiques éventuellement nécessaires : contrat juridique de fédération dans un contexte B2B, réponses aux cinq principes clés de la CNIL (finalité, pertinence, conservation, droit, sécurité), conformité RGPD et analyses d'impacts sur la vie privée des utilisateurs. De même, selon la nature et la visibilité du projet, il faudra anticiper l'implication de la direction générale et des équipes marketing et/ou digitales.

D'un point de vue technique, il est important de s'assurer de la maîtrise de la gestion des certificats électroniques, nécessaires aux fonctions de signature, chiffrement, SSL, etc., qui seront utilisés lors de la mise en œuvre technique du projet. Le risque d'utiliser telle ou telle solution technique et son impact sur les applications sont également à évaluer à ce stade : compatibilité avec tel ou tel protocole de fédération, adaptations nécessaires, etc.

Pendant les spécifications fonctionnelles et techniques

Il faudra définir en détail en particulier :

- les rôles de fédération qui vont être joués : fournisseur d'identités, fournisseur de service, et par qui ;
- la technologie de fédération sur laquelle l'entreprise souhaite s'appuyer :
  - les protocoles de fédération : SAMLv2, OAUth2 ;
  - les applications à intégrer ;
  - les kits de raccordement : Java, .Net, Spring, etc.
- les cinématiques à mettre en œuvre : « IdP Initiated », « SP Initiated », etc. ;
- les éléments techniques à prendre en compte : profils de fédération ;
- les informations qui seront transmises d'un partenaire à l'autre, dans l'assertion SAML par exemple ;
- dans le cas d'une fédération avec O365, par exemple, la méthode de remontée des utilisateurs côté O365.

En complément, cf. annexe « IX.3.3. Questions spécifiques au WebSSO et à la fédération d'identités », section « Cas particulier : application compatible SAMLv2 ».

Pendant la phase de réalisation

Dans le cas d'une fédération B2B, nécessitant des opérations du côté du (ou des) partenaire(s) de fédération, il faudra s'assurer du suivi des opérations techniques associées, notamment de l'application des prérequis côté partenaires, des tests d'interopérabilité, etc.

Pendant la phase de recette

Pas de spécificité particulière.

Pendant la phase de déploiement

Le monitoring de la plateforme de production à l'ouverture du service permettra de s'assurer de la bonne adhésion des utilisateurs à ce nouveau service et d'anticiper les actions correctives éventuelles.

5	***Points clés pour réussir la mise en place d'un tel projet***

Les recommandations sont les mêmes que celles de la fiche « SSO » du chapitre VI.2.1.

VI.2.3. Fiche « Authentification forte »

Note : A la date de rédaction de ce document, un certain nombre de notions ne sont pas suffisamment matures ou déployées pour être développées ici. Elles pourront faire l'objet d'une mise à jour ou d'une extension de ce document. Il s'agit notamment des notions de « Risk Based Authentication », « Adaptive authentication » et de tout ce qui est relatif aux initiatives FIDO, Windows Hello ou Apple TouchID.

« Authentification forte »				
Budget	**Complexité fonctionnelle**	**Complexité technique**	**Durée de mise en œuvre**	**Visibilité**
★★★	★	★	★	★★★

1	***Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?***

Exemples d'arguments	*Interlocuteur(s) concerné(s)*

• **Sécurité**
  • renforcer les mécanismes d'authentification sur les applications et/ou sur les postes de travail, notamment les plus sensibles ;
  • adapter le niveau d'authentification au contexte utilisateur, par exemple s'il est dans le réseau de l'entreprise ou hors de ce réseau ;
  • garantir un bon niveau d'authentification sur les périphériques mobiles ou pour les accès distants ;
  • identifier les utilisateurs qui accèdent à des postes partagés, ou « kiosque », démarrés sur une session Windows générique.
	RSSI

• **Conformité**
  • pour un acteur du monde de la Santé, être en conformité avec le décret de confidentialité et déployer la carte « CPS » pour les professionnels de santé ;
  • pour un acteur du monde bancaire, répondre aux exigences de la norme PCI DSS, en intégrant l'authentification à deux facteurs pour les accès distants au réseau par les employés, les administrateurs et les tiers ainsi que pour l'accès local pour les administrateurs depuis la version 3.2 de 2016 ;
  • pour un OIV, respecter les règles de sécurité de la LPM, notamment celles relatives à la protection des systèmes : règles 11 à 19, dont l'authentification.
	RSSI
	Responsable conformité

• **Coûts d'administration** • alléger la gestion des mots de passe et leur renouvellement ;	Direction financière

• **Ergonomie**
  • remplacer les mots de passe par un moyen d'authentification plus ergonomique et adapté aux usages des utilisateurs ;
  • mettre en place des mécanismes de déverrouillage/verrouillage rapides sur les postes de travail ainsi que de changement rapide d'utilisateur, sur les postes partagés ou « kiosque » notamment ;
  • prendre en compte les derniers standards intégrant l'usage de la biométrie, notamment Microsoft Windows Hello, Apple TouchID.
	Utilisateurs

Cas clients / origines de certains projets (exemples vécus) :

Cas client 1 : #Média #PostesPartagés #ComptesGénériques #300Users

- Déclencheur : Protection contre le vol de données sensibles sur des postes partagés.
- Objectifs principaux : Contrôler et auditer les accès de prestataires externes qui utilisent temporairement des postes partagés démarrés sur une session Windows générique et manipulent éventuellement des informations plus ou moins sensibles.
- Solution : Déploiement d'une solution d'authentification forte et enterprise SSO sur les postes de travail partagés ; authentification sur le poste de type RFID + mot de passe par l'utilisation du badge d'accès aux locaux et de lecteurs sans contact installés sur les postes concernés. La session Windows reste générique.

Cas client 2 : #Santé #Itinérance #Biométrie #5000Users

- Déclencheur : Amélioration de la sécurité et de l'ergonomie sur certains services stratégiques : urgences, blocs opératoires, soins intensifs, pédiatrie, secrétariat médical.
- Objectifs principaux : Augmenter la sécurité sur les postes médicaux en libre-service ; amener de la fluidité aux utilisateurs ; ne plus perdre de temps à saisir des mots de passe ou à le réinitialiser en cas d'oubli, ceci sur les postes personnels, partagés ou mobiles et pour des applications institutionnelles critiques internes ou externes.
- Solution : Déploiement d'une solution d'authentification biométrique de type « *MatchOnServer* » couplée à une solution globale de SSO fournissant des fonctions d'enterprise SSO sur les portables médicaux « kiosques », avec itinérance de session, de WebSSO et d'une solution de fédération SAML pour les accès ou les applications externes.

Cas client 3 : #Energie #Web #OTP #55kUsers

- Déclencheur : modernisation du SI en introduisant de nouvelles technologies et de nouveaux usages : équipements mobiles, personnels, accès externes, applications Cloud.
- Objectifs principaux : Réduire les risques liés à une gestion hétérogène des accès, simplifier l'expérience utilisateur, réduire les coûts.
- Solution : Déploiement d'un « broker d'authentification » composé d'un service d'authentification forte basé sur un token logiciel multi-device en mode SaaS et d'une solution de WebSSO et Fédération d'identités en mode on-premise.

2	*Comment vendre le projet en interne ?*

Avec l'aide d'un PoC, ou d'un pilote

- Comme pour le cas précédent – cf. fiche SSO – la mise en place d'un PoC permet de pratiquer les solutions, de les évaluer et de s'assurer de leur adéquation avec ses propres usages en matière d'ergonomie, de sécurité, de robustesse, etc.
- Si le choix de la technologie à évaluer n'est pas arrêté, il est possible d'en profiter pour évaluer plusieurs méthodes d'authentification. De même, il peut être nécessaire, dans certains cas, d'évaluer des solutions en mode Web, poste de travail (Credential Provider) ou mobile sur smartphones et/ou tablettes.
- Cette démarche de PoC peut provoquer un « effet Waouh » auprès des décideurs et financiers du projet, ce qui en facilitera le financement. Elle peut aussi déboucher facilement sur un pilote, en conditions réelles, sur une population réduite d'utilisateurs, avant un déploiement généralisé et maîtrisé.

Par l'utilisation d'éléments déjà utilisés ou déployés en interne

- Il n'est pas rare de pouvoir mutualiser certaines solutions. Par exemple, lorsque des badges sans contact sont déjà utilisés pour le contrôle d'accès physique, la cantine et/ou le parking, il est souvent possible de les utiliser pour l'authentification sur le poste de travail, les applications et le contrôle d'accès logique. Ceci en combinant l'identification sans contact avec un code PIN par exemple. Dans ce cas, la logistique, c'est-à-dire les badges, le CMS ou le processus de génération et de remise, est déjà maitrisée et les acquisitions matérielles se limitent alors généralement aux lecteurs sans contact.
- Il est également possible de considérer que tout le monde possède aujourd'hui un smartphone, plus ou moins géré par l'entreprise selon les cas, mais que de fait, les solutions s'appuyant sur ce matériel seront simples à déployer.

En associant le projet d'authentification forte à un projet de SSO

- Ces deux projets sont très souvent associés, le premier apportant la sécurité, le second l'ergonomie. Cf. fiche précédente « SSO » pour plus de précisions.

3	*Quels sont les éléments à prendre en compte dans le budget du projet ?*

Les coûts d'acquisition et récurrents ne sont pas les mêmes selon la technologie d'authentification à déployer. Quelques exemples ci-dessous :

- Pour déployer des cartes à puces avec certificat, il faudra des cartes, des lecteurs, un middleware, un CMS, des imprimantes si la personnalisation est souhaitée, une PKI, etc.
- Envisager une offre clé en main de type SaaS peut être une alternative selon sa capacité à absorber ces coûts et notamment celui d'exploitation. Dans le cas de cartes de type RFID ou NFC, sans certificat, il faut considérer la réutilisation d'un circuit logistique déjà existant : est-ce qu'il existe déjà des badges dans la société ? un CMS ? etc.
- Pour une technologie s'appuyant sur un OTP transmis par SMS, il faut être attentif au coût des SMS.
- Pour des solutions à base de biométrie, et au-delà du choix des capteurs, c'est le processus d'enrôlement des utilisateurs qui peut être coûteux. De même, certains utilisateurs peuvent ne pas avoir d'empreinte. C'est le cas par exemple des personnes en milieu médical manipulant des produits corrosifs depuis longtemps. Ceci peut nécessiter la mise en place de solutions alternatives.

De fait, dès qu'un choix de technologie à base de support physique est fait, il est nécessaire de prévoir un stock de secours ou de remplacement pour pallier une défaillance matérielle, la perte ou l'oubli du support. De manière générale, il faut ainsi prévoir, dès le début, les modes dégradés en cas d'indisponibilité du moyen principal d'authentification.

Ensuite, il faut avoir conscience qu'un projet d'authentification forte va souvent de pair avec un projet de SSO. Il faut donc bien borner les frontières de son projet et s'assurer que les solutions choisies sont en adéquation avec le périmètre défini (cf. fiche SSO précédente).

Enfin, la conduite du changement n'est surtout pas à négliger pour les utilisateurs comme les administrateurs.

L'annexe 4 propose une synthèse des éléments à prendre en compte lors de l'évaluation d'une ou plusieurs technologies d'authentification.

4 Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger

Pendant le cadrage / démarrage

Une attention particulière doit être portée dès le départ sur un certain nombre de points :

- s'assurer que la (les) technologie(s) d'authentification choisie(s) est (sont) en adéquation avec les différents usages au sein de l'organisation, c'est-à-dire avec tous les cas d'utilisation pour tous les utilisateurs ;
- s'assurer que la (les) technologie(s) d'authentification choisie(s) est (sont) en adéquation avec ce qui a motivé le projet à l'origine : sécurité, ergonomie, réduction des coûts ou autres ;
- vérifier qu'il n'existe pas d'obstacle majeur, comme les contraintes de la CNIL par exemple, dans le cas de l'utilisation d'authentification biométrique ;
- prévoir les modes dégradés, en cas - par exemple - de carte perdue, de code PIN ou de mot de passe oublié, d'un réseau défaillant qui empêcherait l'envoi et/ou la réception de SMS ou de mail, de matériel cassé ou manquant, de batterie de téléphone vide, etc. ;
- repréciser quel est le périmètre du projet :
  - en terme d'utilisateurs : tous ? seulement un sous-ensemble ? comment sont-ils différenciés ? quels référentiels d'identités sont utilisables ? *Attention sur ce dernier point, car s'il n'existe pas de référentiel d'authentification, il sera peut-être nécessaire de le mettre en œuvre. Cf. fiche « Annuaire » ci-après dans le présent document ;*
  - en terme d'applications, de postes de travail, d'accès : internes ? externes ?
  - en terme de déploiement : définir un périmètre restreint pour le pilote puis l'étendre par exemple.

Pendant les spécifications fonctionnelles et techniques

A définir dans le détail en particulier :

- le processus d'enrôlement et de délivrance des moyens d'authentification aux utilisateurs ;
- la définition des cinématiques d'authentification et des modes dégradés associés.

Pendant la phase de réalisation
Pas de spécificité particulière.
Pendant la phase de recette
Pas de spécificité particulière.
Pendant la phase de déploiement
Il est préférable de déployer une solution d'authentification forte par itération, en commençant en particulier par une phase pilote à l'échelle d'un service, d'une entité, ou d'un sous-ensemble d'utilisateurs par exemple, en tenant compte de leur périmètre applicatif. La mise en place d'indicateurs de pilotage est également recommandée : • retour d'expérience des utilisateurs : adoption ? rejet ? niveau de satisfaction ? • statistiques au niveau du helpdesk : assistance, dépannage, renouvellements, etc.

5 Points clés pour réussir la mise en place d'un tel projet

Quelques points clés :

- considérer la sécurité ET l'ergonomie : le curseur n'est pas évident à positionner entre ces deux notions, mais il est pourtant indispensable de préciser cette position ;
- penser aux modes dégradés et aux solutions de secours en cas de défaillance du moyen principal d'authentification ;
- considérer tous les usages des utilisateurs et s'assurer que les moyens d'authentification forte retenus ne seront pas contre-productifs ;
- se méfier des effets de mode et s'assurer de la pérennité et de la couverture fonctionnelle et technique de certaines solutions très attractives de prime abord ;
- faire attention aux coûts cachés des solutions d'authentification forte. Cf. les éléments relatifs au budget du projet plus haut dans ce document ;
- ne pas négliger les phases d'enrôlement des utilisateurs, ni la conduite du changement, car elles peuvent être coûteuses et complexes à gérer ;
- déployer la solution par itération, et mesurer ce déploiement en ajustant si besoin.

VI.3. Identity management / Gestion des identités

VI.3.1. Fiche « Annuaire d'identités »

« Annuaire d'identités »				
Budget	**Complexité fonctionnelle**	**Complexité technique**	**Durée de mise en œuvre**	**Visibilité**
★★	★★	★	★	★★★

1	***Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?***

Exemples d'arguments	*Interlocuteur(s) concerné(s)*

• **Urbanisation du système d'information**
  • constituer un référentiel central, unique et fiable, pour tous les autres référentiels ou applications du SI ;
  • satisfaire aux prérequis à la mise en œuvre de services liés à la notion d'identité : gestion des identités, des habilitations – Cf. fiches suivantes.
	DSI
	Urbanistes du SI
	Architectes

• **Sécurité**
  • disposer d'un annuaire central pour fédérer les identités ;
  • préparer sa gestion centralisée des accès et son annuaire d'authentification. Cf. fiche « Gestion des habilitations » et fiches « Access Management ».
	RSSI
	DSI

• **Services utilisateurs** • mettre à disposition des services de pages blanches d'entreprise, organigrammes, et localisation géographique des collaborateurs.	Tous

Cas clients / origines de certains projets :

Cas client 1 : #Federation #Social #SItransverse #20kUsers

- Déclencheur : Besoins de consolidation d'informations et nécessité de déployer un service global et homogène pour les différentes organisations membres de la fédération.
- Objectifs principaux : Fournir une gestion unique de l'identité pour toutes les applications du SI transverse et commun aux différents organismes de la fédération, ayant chacun de quelques centaines à quelques milliers d'utilisateurs sur leur SI local ; rationaliser les annuaires associés au SI transverse.
- Solution : Mise en place d'un référentiel central des identités fournissant un service d'authentification pour les applications nationales du SI transverse, ainsi qu'une gestion des habilitations de premier niveau, une administration déléguée, une alimentation automatique et des fonctions de « pages blanches » pour la fédération.

Cas client 2 : #Energie #Intranet #300filiales #90kUsers

- Déclencheur : Mise en service de la nouvelle plateforme Intranet du Groupe.
- Objectifs principaux : Synchroniser les données des annuaires du Groupe ; gérer l'accès des utilisateurs au projet SAP Groupe ; permettre la construction d'un intranet groupe et d'un annuaire exhaustif pages blanches / pages jaunes du Groupe qui soit accessible à tous. Ceci pour une vision globale des 300 sociétés et de 90 000 employés communicants.
- Solution : Mise en œuvre d'un annuaire consolidé et d'une base d'authentification unique pour les applications Groupe dont notamment le portail intranet Groupe. Ceci avec des fonctions de provisioning, de réconciliations, de pages blanches et pages jaunes.

Cas client 3 : #UtilitePublique #Profession #Reglementee #55kUsers

- Déclencheur : Fourniture d'un identifiant unique à la profession, mais également à ses partenaires et aux internautes, et création d'un portail centralisé d'accès aux applications de la profession.
- Objectifs principaux : Unifier et sécuriser l'accès aux services applicatifs ; disposer d'un référentiel complet des membres de la profession ; décloisonner le SI existant ; fédérer et moderniser les outils informatiques de la profession et adresser à terme le grand public.
- Solution : Mise en œuvre d'un annuaire central des identités des utilisateurs de la profession, des partenaires et du grand public, d'un socle d'un système d'identification et d'authentification, et d'un portail centralisé d'accès aux applications de la profession.

2	***Comment vendre le projet en interne ?***

En développant rapidement une offre de services à valeur ajoutée pour les utilisateurs ou les métiers : annuaire intranet, trombinoscope, organigramme, self-service, etc.

En illustrant avec des cas d'usages répondant à un besoin ponctuel fort ou lié à un projet stratégique.

3	***Quels sont les éléments spécifiques à prendre en compte dans le budget du projet ?***

Un projet d'annuaire d'identités peut être associé à des coûts indirects ou périphériques selon le périmètre du projet et le contexte dans lequel il va s'installer par :

- le développement des interfaces avec les autres référentiels pour les alimentations amont et aval ;
- le travail induit sur la mise en qualité des données qui peut être conséquent, exiger beaucoup d'actions préalables et mobiliser fortement les maîtrises d'ouvrage ;
- la gestion du changement avec, éventuellement, l'abandon des référentiels et/ou des processus existants ;
- la réécriture d'applications pour utiliser le nouvel annuaire plutôt que les référentiels existants.

4	***Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger***

Pendant le cadrage / démarrage

Il est impératif à ce stade de :

- bien cadrer le périmètre cible concernant les identités et les attributs à gérer dans l'annuaire ;
- s'attacher à définir la notion d'identifiant de l'identité avec une clé primaire ;

- déterminer les modes d'alimentation et de mise à jour de l'identité : automatismes, transactions de saisie manuelle ou autre.

Sur ces bases, il est important d'identifier les éléments qui composent le contexte de départ :

- recenser les différents référentiels existants et leur utilisation ;
- analyser les données en termes de qualité et de sens ;
- identifier les sources autoritaires de chaque donnée ;
- identifier les processus qui consomment et produisent les données ;
- identifier les propriétaires des données.

Pendant les spécifications fonctionnelles et techniques

Le travail sur les données est primordial :

- déterminer l'identifiant qui sera adopté ;
- définir et valider le catalogue des données, comme les attributs ;
- définir les sources autoritaires ;
- identifier les propriétaires et les acteurs ;
- identifier les processus ;
- définir les règles de gestion avec les acteurs concernés.

Pendant la phase de réalisation

Il est conseillé d'avancer par itérations successives et de présenter à l'issue de chacune de ces itérations des maquettes des écrans de gestion ou de publication des données. Cela permet de valider progressivement le développement de la solution avec le client ou l'utilisateur et d'éviter tout effet tunnel.

Pendant la phase de recette

Nous avons vu que les données occupent une place centrale dans ce type de projet. Il est important de travailler sur une qualité et une volumétrie réelles, pour éviter les surprises sur ces aspects en phase de mise en production.

Pendant la phase de déploiement

Il est conseillé de démarrer sur un périmètre restreint, ou le plus visible, pour élargir par la suite.

Il est également important de bien communiquer sur les services mis en place dans ce projet.

5 Points clés pour réussir la mise en place d'un tel projet

L'analyse des données, à savoir leur qualité et leurs sources, est un volet essentiel d'un projet d'annuaire. Elle permet de déterminer le périmètre des données à collecter ou à ajuster, ainsi que les sources autoritaires de ces données.

La qualité des interfaces d'alimentation est également importante pour respecter l'intégrité des données collectées. Attention aux différents cycles de vie des données dans le temps.

VI.3.2. Fiche « Cycle de vie des utilisateurs »

« Cycle de vie utilisateurs »				
Budget	**Complexité fonctionnelle**	**Complexité technique**	**Durée de mise en œuvre**	**Visibilité**
★★	★★	★★	★★	★★

1	***Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?***

Exemples d'arguments	*Interlocuteur(s) concerné(s)*

• **Sécurité**
  • provisionner les identités : créer l'identité des nouveaux arrivants, prendre en compte les mouvements de personnes et les changements de situation, harmoniser les données dans les différents référentiels ;
  • conformité : prendre en compte les mutations et les départs ;
  • faciliter la réalisation d'audits et de contrôles.
	DSI
	Risques et audit
	Métiers
	RSSI

• **Retour sur investissement**
  • diminuer la part des tâches administratives ;
  • remplacer les formulaires « papier ».
	DRH, DAF
	DSI

• **Urbanisation** • disposer d'un annuaire utilisateur à jour et de référence.	DSI Métiers

Cas clients / origines de certains projets :

Cas client 1 : #Habitat #SIRH #2000Users

- Déclencheur : Besoin de mettre fin aux doubles saisies SIRH / SI.
- Objectifs principaux : Récupération des données SIRH pour prendre en compte les événements liés au cycle de vie des collaborateurs ; automatisation de la création des comptes réseau, messagerie et SIRH.
- Solution : Mise en place d'une solution de gestion des identités, avec échange de données pour récupération des événements RH et création des comptes utilisateurs dans le SIRH.

Cas client 2 : #Service #SaaS #5000Users

- Déclencheur : Evolutions du SI avec une croissance du nombre d'applications SaaS et des applications de gestion RH du fait de la dématérialisation des procédures de recrutement et de fin de contrat.
- Objectifs principaux : Suppression des formulaires Excel ; réduction des tâches d'administration des utilisateurs dans plusieurs systèmes ; centralisation et amélioration du contrôle ; préparation de la gestion des habilitations en étape préalable.
- Solution : Mise en œuvre d'une solution de gestion du cycle de vie des utilisateurs.

Cas client3 : #Distribution #3000Users

- Déclencheur : Modernisation du SI et automatisation des mouvements de personnes.
- Objectifs principaux : Optimiser la gestion des mouvements des collaborateurs au sein de l'organisation, fonction anciennement gérés au travers d'une application Notes ; disposer d'un identifiant unique et mettre en place un modèle ORBAC pour préparer la gestion des habilitations ; mettre en place un provisioning automatique sur les référentiels principaux du SI.
- Solution : Mise en œuvre d'une solution de gestion du cycle de vie des utilisateurs avec un référentiel centralisé, un processus de gestion des flux d'entrée / mobilité / sortie, un provisioning amont et aval.

2	***Comment vendre le projet en interne ?***

En mettant en avant :

- l'efficacité et la réactivité de la prise en compte des événements RH : arrivée, mutation, départ, etc. ;
- la réutilisation des données RH : pas de saisie des mêmes éléments à différents points du SI ;
- la réduction des erreurs de saisie, et donc l'amélioration de la fiabilité des données.

3	***Quels sont les éléments spécifiques à prendre en compte dans le budget du projet ?***

La gestion du cycle de vie des utilisateurs consomme des informations en provenance du SIRH et d'autres référentiels. Le travail sur la qualité des données est nécessaire pour disposer d'une base fiable et permet de bien connaître la nature, l'utilisation et la signification de chaque donnée dans les référentiels amont.

Des coûts indirects peuvent donc être induits par :

- la mise en conformité et le nettoyage des données ;
- le développement de connecteurs pour l'extraction de données avec une implication possible des éditeurs ;
- la supervision des échanges de données et la reprise sur incidents, particulièrement si une partie du SI est externalisée ;
- les ajustements sur les processus métier d'entrée/sortie/mutation qui n'auraient pas été traités de manière exhaustive dans la première version du projet.

4	***Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger***

Pendant le cadrage / démarrage

- Mettre à plat des processus RH liés au cycle de vie de l'utilisateur. Il faut tous les lister, quitte à ne pas forcément tous les implémenter tout de suite :
  - arrivée d'internes, d'externes, en CDI, en CDD, de prestataires, de stagiaires, d'intérimaires ou d'autres cas ;
  - modification : changement de fonction, de structure, de nom, de hiérarchie, etc.
  - départ : congés longue durée, arrêt maladie, fin de mission, fin de prestations, fin de marché, etc.
- Analyser la qualité des données SIRH : la même donnée peut avoir une valeur différente selon le sens qu'on lui donne et le contexte d'utilisation : RH, métier, etc.

- Construire un référentiel ou catalogue des données liées aux processus.

Pendant les spécifications fonctionnelles et techniques

- Associer les ressources humaines à l'analyse et au pilotage.
- Valider les différents processus et flux liés aux événements RH et identifier quels en sont les acteurs.
- Valider, avec les directions métiers, le catalogue des données liées à l'identité et aux attributs de la personne dans l'organisation.
- Identifier les différents états possibles de l'identité : inactive, active, archivée, et prévoir la gestion des changements d'état.
- Identifier les cas aux limites : renouvellement de contrats, remplacement d'arrêt maladie, double contrat, période de biseau, double immatriculation, etc.

Pendant la phase de réalisation

- Procéder au plus tôt par itération pour valider les processus.

Pendant la phase de recette

- Dérouler les processus et les cas identifiés lors des phases amont avec des données identiques à la production en qualité et volumétrie.

Pendant la phase de déploiement

- Partir, si cela est possible, sur un pilote avant de généraliser le déploiement, sachant que toutes les solutions et/ou configurations ne le permettent pas.
- Organiser la remontée d'information du terrain pour identifier les cas particuliers.

5 Points clés pour réussir la mise en place d'un tel projet

Quelques points clés :

- travailler avec les RH sur les données et les processus ;
- élaborer un catalogue des données, une cartographie des processus ;
- démontrer le gain en termes d'efficacité, de fiabilité et de ressources ;
- se doter de moyens pour piloter le service rendu et mesurer la qualité des données fournies par les sources d'alimentation.

VI.3.3. Fiche « Gestion des habilitations »

« Gestion des habilitations »				
Budget	**Complexité fonctionnelle**	**Complexité technique**	**Durée de mise en œuvre**	**Visibilité**
				

1	***Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?***

Exemples d'arguments	*Interlocuteur(s) concerné(s)*

• **Sécurité**
  • maîtriser et tracer l'allocation, la modification et le retrait des droits des utilisateurs sur le SI ;
  • produire des rapports sur les habilitations permettant de savoir qui a accès à quoi ;
  • contrôler le retrait des droits et désactiver automatiquement les comptes après la date de départ de l'utilisateur ;
  • sensibiliser les valideurs impliqués dans l'attribution de droits ;
  • réduire le risque opérationnel lié à l'utilisation de processus manuels ;
  • protéger le secret industriel grâce au contrôle des droits
	RSSI
	Risque
	Conformité
	DSI

• **Audit / Conformité**
  • répondre aux contraintes du contrôle interne, des régulateurs, des commissaires aux comptes ou autres autorités de tutelles ;
  • faciliter les revues d'habilitations. Cf. fiche « revues d'habilitations » ;
  • permettre le contrôle du respect du principe de la SoD.
	RSSI
	Risque
	Conformité
	Finance / DAF

• **Urbanisation**
  • disposer d'un annuaire et référentiel utilisateur à jour ;
  • disposer d'un référentiel central d'habilitations pour les applications.
	DSI
	Urbanistes du SI
	Architectes

• **Confort / fonctionnalités / services**
  • fournir du confort aux utilisateurs via des procédures automatisées ;
  • gérer les habilitations sur les applications Cloud/externes ;
  • offrir un portail self-service de demande d'accès à des applications du SI.
	DSI
	Utilisateurs

• **Retour sur investissement**
  • améliorer l'efficacité et la fiabilité des processus d'habilitations ;
  • automatiser le provisionnement des comptes et des droits dans le SI ;
  • supprimer les processus utilisant des formulaires « papier ».
	DAF
	DRH
	DSI

Cas clients / origines de certains projets :

Cas client 1 : #Finance #Règlementation #5kUsers

- Déclencheur : Refonte des procédures de la gestion des habilitations.
- Objectifs principaux : Formaliser le processus d'habilitation ; missionner des propriétaires du SI ; respecter le principe du moindre privilège ; obtenir une vision consolidée des habilitations d'une personne ; gérer efficacement les mobilités ; assurer la traçabilité de la gestion des habilitations ; contrôler les habilitations ; sensibiliser les utilisateurs et les acteurs de la gestion des habilitations.
- Solution : Mise en place d'un référentiel central des habilitations et des systèmes applicatifs ; nomination des acteurs, à savoir les propriétaires et délégataires, les correspondants habilitations, etc. ; définition des procédures et automatisation ; mise en place de la revue des droits.

Cas client 2 : #Media #TurnOver #10kUsers

- Déclencheur : Nécessité de gérer les habilitations des différents utilisateurs du Groupe : CDI, CDD, intérimaires, intermittents, stagiaires, prestataires externes, dont certains avec un fort turn-over.
- Objectifs principaux : Simplifier et sécuriser les processus d'attribution des droits à l'ensemble du SI ; apporter un gain de temps non négligeable dans l'administration de ces tâches ; offrir des nouveaux services aux utilisateurs dont le self-service notamment ; être en conformité avec les réglementations en vigueur.
- Solution : Mise en œuvre d'une solution de gestion du cycle de vie des utilisateurs et de leurs habilitations sur le SI basée sur un modèle de droits, avec un processus des flux d'allocation de droits et un provisioning automatique vers les applications du SI.

Cas client 3 : #Habitat #SIRH #2000Users

- Déclencheur : Outil de gestion des habilitations spécifique et difficile à maintenir ou à faire évoluer.
- Objectifs principaux : Reprendre le périmètre existant de la gestion des habilitations ; abandonner les formulaires envoyés par courriel ; réduire les délais de traitement.
- Solution : Mise en place d'une solution de gestion des habilitations dans laquelle les demandes sont directement exprimées et traitées, avec des informations récupérées à partir du SIRH et des référentiels secondaires.

Cas client 4 : #Santé #Audit #40kUsers

- Déclencheur : Audit sécurité par l'ANSSI.
- Objectifs principaux : Répondre à la difficulté de disposer de la possibilité d'auditer les accès des utilisateurs ; garantir que seuls des médecins accèdent aux dossiers des patients ; pouvoir informer de façon fiable le patient des accès à son dossier ; disposer d'alertes en cas d'accès illicite à un dossier.
- Solution : Tenue d'une matrice d'habilitations ; automatisation des contrôles de cohérence des droits affectés en fonction des métiers ; processus de maîtrise de la matrice d'habilitations ; contrôles mensuels des comptes pour procéder à la fiabilisation du dispositif.

2	*Comment vendre le projet en interne ?*

Démontrer le besoin : faire un audit des habilitations, même sur un périmètre restreint, comme les applications sensibles par exemple, pour montrer les écarts et les risques.

Démontrer le retour sur investissement : quelques cas d'usages permettent en général d'identifier des leviers en termes de coût, de délai, de qualité.

3	*Quels sont les éléments spécifiques à prendre en compte dans le budget du projet ?*

Il est nécessaire de tenir compte des coûts spécifiques suivants :

- coût de refonte des applications : par exemple, pour un projet de gestion des habilitations comprenant une mise en œuvre de la SoD, si le modèle de droits interne aux applications ne respecte pas lui-même la SoD ;
- cartographie des applications et revue des profils applicatifs et des rôles métier ;
- conduite du changement, notamment pour les acteurs de la cellule habilitation ou les managers qui allouent les droits ;
- coûts d'un POC.

4	*Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger*

Pendant le cadrage / démarrage

- Identifier le sponsor du projet : le projet doit être porté à un haut niveau et doit avoir suffisamment de poids de manière transverse : COMEX, DAF, etc.
- Définir le périmètre du projet et la roadmap de déploiement :
  - Quelles applications ? Les plus sensibles ? Les plus utilisées ?
  - Quelles filières métier ?
- Identifier les acteurs impliqués dans le projet :
  - RH, plus dans l'optique de les sensibiliser ;
  - Propriétaires/responsables d'applications, responsables des allocations de droits, acteurs des processus d'allocation. Ils sont indispensables dans l'analyse des données.

Pendant les spécifications fonctionnelles et techniques

- Pour la définition des rôles, identifier toutes les sources :
  - gestionnaires d'application ;
  - responsables de processus ;
  - personnes dans l'organisation qui incarnent un rôle ;
  - personnes « qui savent ».
- Appliquer une approche itérative pour confronter la réalité avec la simulation. A ce stade un outil peut aider.
- Mixer les approches « Top/down » et « Bottom/Up » dans l'analyse.

- Mettre en œuvre une maquette pour les aspects concrets.
- Effectuer une analyse détaillée sur :
  - les données : qualité, relations, cycle de vie ;
  - les processus : identifier les cas possibles, même aux limites, avec les responsables d'applications, les métiers.

Pendant la phase de réalisation

Procéder au plus tôt par itération pour valider les processus.

Pendant la phase de recette

Pas de spécificité particulière.

Pendant la phase de déploiement

- Implémenter le modèle, puis déployer par vagues ou lots : attention aux limitations de certaines solutions dans ce domaine (Cf. intérêt du POC).
- Prévoir une formation poussée des responsables d'allocation des droits et assurer le support.
- Avoir un COPIL qui suit l'avancée du déploiement.
- Organiser la remontée d'informations du terrain pour identifier les cas particuliers qui n'auraient pas été rapportés dans l'analyse et les anomalies ou points de blocage pour les corriger.

5 Points clés pour réussir la mise en place d'un tel projet

Dans la conduite du projet, il faut :

- avoir un bon sponsor et pilote du projet ;
- impliquer les métiers dès le début du projet ;
- impliquer les RH au sens d'une sensibilisation ;
- travailler rapidement sur les données réelles / terrain ;
- valider la qualité des données, leur cohérence, les liens entre les différents référentiels existants.

Penser à lotir et déployer son projet par vagues, en :

- priorisant les applications selon la maturité de la filière métier et la cohérence d'utilisation du périmètre applicatif ;
- mettant l'accent sur les applications stratégiques du point de vue de la visibilité ou à forte activité en terme de gestion des habilitations pour être en situation de « quick win ».

Enfin, dans le choix d'une solution, il est conseillé de :

- réaliser un POC en amont pour valider les principes de fonctionnement, les possibilités intrinsèques de la solution : connecteurs, modalités de déploiement, personnalisation des processus, etc. ;
- accepter de se faire accompagner pour éviter les écueils.

VI.4. Gouvernance des Identités et des Accès

VI.4.1. Fiche « Revue des habilitations / Recertification »

<table>
<tr><th colspan="5">« Revue des habilitations / Recertification »</th></tr>
<tr><th>Budget</th><th>Complexité fonctionnelle</th><th>Complexité technique</th><th>Durée de mise en œuvre</th><th>Visibilité</th></tr>
<tr><td>  </td><td>  </td><td>  </td><td>  </td><td>  </td></tr>
<tr><td>1</td><td colspan="4">Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?</td></tr>
<tr><td colspan="4">Exemples d’arguments</td><td>Interlocuteur(s) concerné(s)</td></tr>
<tr><td colspan="4">• Sécurité / diminution des risques opérationnels
  • supprimer les comptes orphelins ;
  • s’assurer de la bonne fermeture des comptes pour les personnes parties ;
  • s’assurer que chaque personne possède bien le minimum de droits suffisants et nécessaires sur le SI ;
  • contrôler les droits sur les comptes génériques et leur association aux personnes physiques ;
  • s’assurer, pour chaque application et chaque ressource, que seules les personnes autorisées peuvent y accéder, et selon leur fonction.</td><td>RSSI
Contrôle interne
Risques</td></tr>
<tr><td colspan="4">• Audits réglementaires ou d’organes de tutelle
  • fournir des preuves de revues ;
  • fournir des preuves de suivi de plan d’actions post-revues.</td><td>DAF
DG</td></tr>
<tr><td colspan="4">• Lutte contre la fraude
  • s’assurer du non-cumul de droits toxiques.</td><td>DAF
Risques</td></tr>
<tr><td colspan="4">• Coûts
  • réduire le coût des licences applicatives en s’assurant que les comptes inutiles sont supprimés.</td><td>DSI
DAF</td></tr>
<tr><td colspan="5">Cas clients / origines de certains projets :</td></tr>
<tr><td colspan="5">Cas client 1 : #finance #sécurité #>5kUsers
• <u>Déclencheur</u> : Audits réguliers de la société mère.
• <u>Objectifs principaux</u> : Gagner du temps sur les revues et les réponses aux audits, maîtriser les habilitations.
• <u>Solution</u> : Démarrage d’un projet IAG complet incluant la revue des processus de gestion des identités et des accès mais également la mise en œuvre d’un module de revue des habilitations.</td></tr>
</table>

Cas client 2 : #énergie #conformité # >40kUsers

- Déclencheur : Audit des commissaires aux comptes.
- Objectifs principaux : Maîtriser les habilitations et éviter les combinaisons de droits toxiques (SoD – Segregation of Duty / séparation des tâches) sur le SI finance.
- Solution : Mise en place d'un dispositif de contrôle des habilitations et des droits toxiques sur le SI finance.

Cas client 3 : #assurance #sécurité #>5kUsers

- Déclencheur : Certification ISO 27001.
- Objectifs principaux : Réaliser des rapports de revues sur le périmètre des actifs sensibles identifiés et suivre les plans d'actions de corrections.
- Solution : Mise en place d'un dispositif de contrôle des habilitations sur l'ensemble des actifs sensibles avec des revues réalisées à la fois sur un axe organisationnel et sur l'axe des actifs ; outillage des revues avec une solution du marché.

Cas client 4 : #banque #sécurité #>2kUsers

- Déclencheur : Audits des commissaires aux comptes et audits de la société mère.
- Objectifs principaux : Maîtriser les habilitations ; éviter les combinaisons de droits toxiques sur l'ensemble des actifs sensibles ; mettre en œuvre de la SoD.
- Solution : Mise en place d'un dispositif de contrôle des habilitations sur l'ensemble de l'organisation pour les actifs les plus sensibles ; outillage des revues avec une solution du marché.

Cas client 5 : #service #sécurité #>20kUsers

- Déclencheur : Analyse de risques et décision de réduire les risques opérationnels.
- Objectifs principaux : Effectuer des revues sur les comptes à privilèges, sur l'ensemble des organisations et sur les actifs jugés sensibles.
- Solution : Mise en place d'un dispositif de contrôle des habilitations sur l'ensemble des actifs sensibles avec des revues réalisées à la fois sur un axe organisationnel et sur l'axe des actifs. Outillage sur une partie des revues avec pour objectif de remplacer à terme les revues manuelles.

2	***Comment vendre le projet en interne ?***

En réalisant un audit flash

- Démontrer en quelques jours qu'il est possible d'obtenir rapidement la liste des comptes orphelins, des personnes possédant le plus de droits, ou des personnes à la finance possédant des droits à privilèges. Ceci permet de sensibiliser les principales parties prenantes.
- Dans le cadre d'un tel audit flash il est indispensable de disposer d'extractions brutes des référentiels des habilitations et d'un référentiel des identités : fichier RH, fichier des externes, etc. afin que les résultats soient significatifs et parlants.
- L'audit flash permet également la mise à disposition de rapports prêts à l'emploi pour les différentes populations : auditeurs, responsables d'actif, managers d'organisation, etc.

En mettant en avant des gains opérationnels

- Les revues et le suivi des plans d'actions sont souvent chronophages pour les personnes impliquées : manager, responsable d'actifs, responsable de la revue, responsable des actions de corrections. La mise en avant des gains opérationnels fournis par de l'outillage est un des arguments les plus utilisés.
- La possibilité offerte, par les outils du marché, de mise à disposition d'une interface intuitive pour les utilisateurs permet de réduire la durée des revues et également d'en améliorer la qualité.
- Parfois, le fait d'organiser les revues effectuées manuellement ici ou là et d'en améliorer « l'outillage manuel » de type Excel ou Access permet également d'obtenir des gains opérationnels significatifs.
- La mise à disposition d'une vue à 360° de l'ensemble des habilitations pour l'ensemble des utilisateurs peut également permettre aux équipes opérationnelles de types Help Desk, infrastructures ou applicatives d'effectuer des dépannages plus efficaces.

En calculant un ROI sur les licences économisées

- Il n'est pas rare d'avoir des audits de licences au sein des DSI qui révèlent un usage de solution plus important qu'il ne devrait l'être en raison d'accès trop larges ou non supprimés. Dans certains cas, la mise en place d'un dispositif de contrôle sur les actifs dont le coût de licences est important peut déboucher sur un gain financier à moyen terme. Cela ne représente cependant pas la majorité des cas.

3	***Quels sont les éléments spécifiques à prendre en compte dans le budget du projet ?***

Outre la mise en place des processus et de l'outillage éventuel qui engendrent classiquement du CAPEX projet et de l'OPEX pour l'exécution du service, ce type de projet peut engendrer des coûts bien particuliers :

- documentation des habilitations : il n'y a pas d'intérêt à demander de revoir des habilitations qui ne sont pas compréhensibles des managers d'organisation ou des responsables d'actifs ;
- construction et maintien d'une matrice de SoD : la SoD n'est pas toujours dans le périmètre de ce type de projet. Mais si tel est le cas, cette activité demande des ressources non négligeables pour sa mise en œuvre et son maintien en condition opérationnelle ;
- industrialisation des extractions : la génération régulière, outillée ou manuelle, des extractions pour alimenter la solution peut engendrer un coût non négligeable. La reproductibilité et l'intégrité des extractions sont deux points essentiels. Les extractions sont plus ou moins complexes à réaliser suivant le type de système de revue : AD, Mainframe, RACF, SAP, etc. ;
- désignation des responsables métier ou des responsables d'actifs : il ne peut pas y avoir de revue sans responsable de revue, que ce soit sur un axe organisationnel ou sur l'axe des actifs. Suivant la maturité de l'organisation, certains acteurs sont plus ou moins difficiles à identifier afin d'effectuer une revue efficace ;
- conduite du changement : la mise en place d'un dispositif de revue implique des acteurs pour les activités liées à cette revue. Les acteurs doivent être sensibilisés et formés, que ce soit pour les revues en tant que telles, ou pour les actions de correction qui s'ensuivent.

4	*Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger*

Pendant le cadrage / démarrage

Il est primordial de définir un périmètre limité, surtout sur une première itération, afin d'avoir les moyens de démarrer le projet, le faire aboutir et pouvoir traiter les plans d'actions de corrections qui en découlent.

Le cadrage doit définir :

- le périmètre des applications et des ressources ;
- le périmètre des organisations et des utilisateurs ;
- le niveau de granularité souhaité pour les revues : comptes, profils, droits fins ;
- les acteurs des revues ;
- les consommateurs des activités liées aux revues.

De plus, il est important de faire la différence entre le contrôle périodique et la surveillance, contre la fraude à un instant T par exemple, au sein du cadrage afin d'éviter des dérives éventuelles du projet.

Pendant les spécifications fonctionnelles et techniques

Il est conseillé de travailler par ateliers thématiques puis par type d'applications et type de ressources :

- ateliers fonctionnels : cas d'usages utilisateurs, cinématiques d'accès aux données, rapports visibles, cinématiques de revue, types de revues, contrôles de qualité, contrôles de conformité, etc. ;
- ateliers techniques : architecture globale, stockage, sauvegarde, archivage, etc. ;
- référentiel des identités et des organisations : sources d'alimentation, règles de transformation et de réconciliation ;
- applications et ressources : type de raccordement, via fichier ou connecteur, corrections automatiques ou manuelles, modèle de données, règles de réconciliations, etc.

Pendant la phase de réalisation

Il est essentiel de réussir ces étapes clés lors de la phase de réalisation :

- qualité du référentiel des identités : pierre angulaire pour les revues de comptes et d'habilitations ;
- qualité du référentiel des organisations : indispensable pour des revues sous un axe organisationnel ;
- qualité du référentiel des responsables d'actifs : indispensable pour des revues par actif ou type d'actif ;
- qualité des rapports, avant de s'attaquer à des rapports de conformité ;
- qualité des règles de réconciliation et finalisation de façon manuelle ;
- traitement de la SoD seulement lorsque les rapports de qualité et de conformité « basiques » sont validés.

Et aussi :

- travailler dans l'ordre : qualité des identités, des applications, des comptes, des droits fins ;
- avoir à l'esprit que les applications sont plus ou moins sensibles ;
- anticiper les taux de rejet et les difficultés de réconciliation et le temps que cela prend ;
- travailler sur la mise en qualité des données ;
- travailler par palier et itérations.

Pendant la phase de recette

La phase de recette nécessite souvent de vérifier des centaines ou des milliers de données. Il est dans ce cas indispensable d'effectuer une recette par palier :

- vérification des données d'identités ;
- vérification des données des actifs : un rapport par actif à valider *a minima* ;
- vérification des règles de réconciliation : de mauvaises règles de réconciliation aboutiront à des revues erronées ;
- vérification des rapports de qualité ;
- vérification des rapports de conformité ;
- vérification des accès aux données.

Pendant la phase de déploiement

Lors de la phase de déploiement il est souvent nécessaire de reprendre des réconciliations manuelles effectuées en phase de réalisation ou de recette afin d'éviter des écarts et un double travail.

Le déploiement en tant que tel ne nécessite pas d'attention particulière, exception faite des droits sur les données. La mise en œuvre d'une première revue sera, quant à elle, à suivre avec précaution, en prenant en compte la conduite du changement et la mobilisation des différents acteurs.

5 Points clés pour réussir la mise en place d'un tel projet

Démarrer « petit et simple » : une fois que le modèle et la brique de base sont construits, le périmètre applicatif sera élargi ainsi que le nombre de rapports. Chaque rapport implique une charge de travail de correction des données lors de son utilisation.

VI.4.2. Fiche « Gestion de rôles »

« Gestion de rôles »				
Budget	**Complexité fonctionnelle**	**Complexité technique**	**Durée de mise en œuvre**	**Visibilité**
				

1	***Pourquoi un tel projet ? Quels avantages et pour qui en priorité ? Quels arguments pour convaincre de démarrer un tel projet au plus haut niveau ?***

Exemples d'arguments	*Interlocuteur(s) concerné(s)*

• **Sécurité et diminution des risques opérationnels**
  • s'assurer simplement que, pour une fonction donnée, seuls les droits nécessaires sont affectés : ajout d'un ou plusieurs rôles correspondant à la fonction ;
  • s'assurer du retrait des anciens droits lors d'une mutation.
	RSSI
	Contrôle interne
	Risques

• **Audits réglementaires ou d'organes de tutelle**
  • disposer d'une documentation justifiée des rôles existants : valideurs, contenu ;
  • répondre à certains audits qui mentionnent simplement de « mettre en place une gestion par rôles », ce qui peut être discutable puisqu'il s'agit plus d'un moyen que d'un but.
	DAF
	DG

• **Lutte contre la fraude** • une matrice de SoD basée sur les rôles est généralement plus facile à maintenir qu'une matrice basée sur des droits fins.	DAF Risques

• **Expérience utilisateur**
  • simplifier les processus d'affectation et de retrait de droits ;
  • simplifier les tâches opérationnelles de revue ;
  • éviter aux exploitants et aux utilisateurs d'avoir à connaître tous les rôles.
	Utilisateurs

Cas clients / origines de certains projets :

Cas client 1 : #assurance #sécurité #>5kUsers

- Déclencheur : Audit d'un organe réglementaire.
- Objectifs principaux : Améliorer la maîtrise des habilitations.
- Solution : Conception des rôles sur la base d'interviews métiers associés à un outillage pertinent, puis intégration des rôles dans les processus outillés de gestion des habilitations. Une phase pilote sur une direction est réalisée avant le déploiement sur l'ensemble de l'organisation. Les rôles sont gérés par la DSI.

Cas client 2 : #banque #sécurité #>2kUsers

- Déclencheur : Recommandation « P1 » lors d'un audit.
- Objectifs principaux : Améliorer la maîtrise des habilitations.
- Solution : Conception des rôles sur la base d'interviews métiers et modélisation à l'aide d'un outillage IAG ; mise en place de la solution IAG avec les fonctionnalités suivantes : gestion des rôles, revues, SoD, puis extension au provisioning et à la gestion des identités. Les rôles sont gérés par la DSI.

Cas client 3 : #service #sécurité #>20kUsers

- Déclencheur : Faciliter le traitement des demandes d'habilitations.
- Objectifs principaux : Réduire le temps de traitement des habilitations : ajouts, modifications et retraits.
- Solution : Conception des rôles sur la base d'interviews métiers et modélisation à l'aide d'un outillage Excel ; mise en place d'une solution IAM avec personnalisation des interfaces pour la prise en charge de la gestion des rôles. Les rôles sont gérés par les métiers.

Cas client 4 : #banque #sécurité #>3kUsers

- Déclencheur : Faciliter le traitement des demandes d'habilitations.
- Objectifs principaux : Conformité des habilitations et efficacité opérationnelle.
- Solution : Conception des rôles sur la base d'interviews métiers et modélisation à l'aide d'un outillage Excel. Mise en place d'une solution IAM avec personnalisation des interfaces pour la prise en charge de la gestion des rôles. Les rôles sont gérés par les métiers.

Cas client 5 : #santé #sécurité #40kUsers

- Déclencheur : Certification des comptes.
- Objectifs principaux : Prouver le bien-fondé des rôles et obtenir la validation du contenu par les MOA.
- Solution : Concevoir les rôles en s'appuyant sur les besoins métiers en normalisant leur construction et leurs structures ; faciliter leur évolution et la compréhension par tous les acteurs ; outillage Excel, circuit de validation par les métiers.

2 Comment vendre le projet en interne ?

La mise en place d'une gestion de rôles est certainement le sujet IAM le plus difficile à vendre. Son ROI est toujours sujet à discussion.

La question à se poser est : « le temps perdu à gérer et maintenir les rôles fait-il réellement gagner du temps et améliore-t-il la qualité des affectations d'habilitations » ?

La réponse dépend de plusieurs facteurs, dont le type d'organisation concernée, la gouvernance mise en œuvre et la modélisation des rôles retenue. Dans les faits, le véritable ROI n'est calculable qu'après quelques années de pratique.

Lorsque la mise en place d'une gestion de rôles s'avère réellement nécessaire, les leviers peuvent être les suivants :

- mise en avant de l'apport de la gestion de rôles pour l'adoption d'une solution de type IAM/IAG auprès des métiers ;
- facilité d'évolution et de compréhension des droits ;

- démonstration des interfaces utilisateurs de gestion des habilitations simplifiées par l'utilisation de rôles ;
- démonstration de la simplification de la matrice de SoD ;
- identification des gains opérationnels et calcul de ROI : temps gagné sur la gestion des affectations par rapport au temps consommé sur la gestion des rôles.

3	***Quels sont les éléments spécifiques à prendre en compte dans le budget du projet***

La modélisation initiale des rôles sur l'ensemble d'un périmètre est généralement coûteuse et nécessite de nombreux allers retours avec le métier. Elle nécessite une connaissance globale forte de l'organisation.

La mise en œuvre d'une gestion de rôles sans outillage est généralement vouée à l'échec du fait de sa complexité de maintenance. Un outillage spécifique est donc à prévoir.

Les rôles sont à revoir régulièrement afin de coller aux métiers et aux réorganisations. Cette « remodélisation » peut être lourde, mais est essentielle. Elle nécessite souvent de revoir les rôles avec les métiers et d'impliquer des personnes rôdées à ce type d'exercice et possédant une expertise pointue.

4	***Etapes clés du déploiement – les questions à se poser et les points à ne pas négliger***

Pendant le cadrage / démarrage

Le cadrage de la gestion des rôles doit répondre aux questions suivantes :

- Quelle modélisation de rôles réaliser ? RBAC ? ABAC ? OrBAC ? etc.
- Quelle organisation et quels processus autour de la gestion des rôles ?
- Quels sont les périmètres organisationnels et applicatifs à couvrir ? Quelle est la roadmap ?
- Les personnels IT doivent-ils être intégrés dans la gestion des rôles ?
- Quel(s) outil(s) utiliser et quels sont ceux impactés ?
- La modélisation des rôles fait souvent apparaître des anomalies dans les applicatifs à intégrer. Dans ce cas, quel est le plan de traitement ?

Pendant les spécifications fonctionnelles et techniques

Il est conseillé de travailler par entité pour la modélisation des rôles. Pour chacune d'elles, un ensemble de rôles doit être défini et confronté à la réalité des référentiels d'habilitations.

Tous les processus et les interfaces utilisateurs autour des rôles doivent être rigoureusement décrits.

Pendant la phase de réalisation

Pour chaque périmètre, il convient d'adopter une approche itérative pour la modélisation des rôles :

- interview des métiers ;
- identification de rôles théoriques par l'analyse de l'organisation et des fonctions ;
- identification de rôles opérationnels par l'analyse de données d'habilitations de chaque contexte ;
- modélisation d'une première version des rôles ;
- validation avec les métiers et ajustements éventuels.

Une fois les modèles de rôles définis, documentés et instanciés, ceux-ci doivent être intégrés au sein des processus workflow opérationnels d'une solution technique.

Pendant la phase de recette

La phase de recette doit être la plus proche possible de la production en utilisant un volume réel de données afin d'évaluer les impacts pour la production. Une recette sur un jeu de données partiel serait catastrophique.

Il convient donc de mettre en place un environnement de recette identique à la production pour ce qui est du périmètre des populations et des habilitations à couvrir.

Pendant la phase de déploiement

Le déploiement de la gestion des rôles est obligatoirement réalisé par lots afin de ne pas perturber les utilisateurs. Sinon il est nécessaire de mettre à disposition une toute nouvelle solution outillée de gestion des habilitations.

5 Points clés pour réussir la mise en place d'un tel projet

Quelques points clés :

- fonctionner par itérations ;
- disposer d'un appui fort ;
- ne pas sous-évaluer les coûts internes et externes de mise en œuvre et de maintien en condition opérationnelle.

VII. Après le projet

Si un projet IAM bien exécuté traduit souvent des spécifications de bonne qualité, un projet IAM « en bonne santé » traduit en général une organisation et un partage des responsabilités sans faille. En effet, un tel projet ne s'arrête pas le lendemain de la mise en production. Négliger l'importance de l'après-projet nuirait à la bonne réussite de ce dernier et à la satisfaction des utilisateurs vis-à-vis de la solution mise en œuvre.

Tant que la solution est en place, elle doit être maintenue et s'adapter aux différentes évolutions dans l'entreprise, qu'il s'agisse d'évolutions techniques ou organisationnelles. C'est une nouvelle étape dans le cycle de vie de la solution, le « mode récurrent ». La transition du mode projet au mode récurrent représente ainsi de nouveaux défis pour l'entreprise. Nous allons les passer en revue dans la suite de cette partie, puis, dans un second temps, nous nous intéresserons à la question du retour sur investissement des projets IAM

VII.1. Les défis du mode récurrent

Après la mise en production d'une solution d'IAM, un certain nombre d'évènements peuvent induire la nécessité de la faire évoluer.

Evolution du périmètre applicatif

Dans le mode récurrent, il faut considérer l'ajout en permanence d'applications dans le périmètre du projet IAM. Lors de la phase initiale, un certain nombre d'applications ont été intégrées. Si la solution mise en place apporte satisfaction, d'autres applications pourront être intégrées par la suite. Il est indispensable de définir le processus de gestion des applications avec, dans l'idéal, un responsable interne en garant de ce processus.

Evolution des habilitations

Les rôles fins d'une application peuvent être modifiés, les rôles métiers peuvent évoluer. Il est nécessaire de suivre ces changements. Le maintien à jour de la matrice des rôles et des habilitations permet d'assurer, à tout moment, l'adéquation des accès entre la théorie et la pratique.

Réorganisation de l'entreprise

L'entreprise ne cesse d'évoluer. Une réorganisation de l'entreprise, interne ou dans le cadre d'une fusion, implique une adaptation de la solution IAM. Par exemple la réorganisation des structures ou de nouveaux sites peut nécessiter la mise à jour des rôles et de la matrice des droits. Ces changements peuvent, dans certains cas, être lourds. Si l'organisation est très agile de ce point de vue, le critère de l'évolutivité doit être un point central du choix de la solution.

Changement sur le SI RH

Le SI RH étant très généralement le référentiel principal sur lequel se base la solution d'IAM, les changements de type évolution de technologie, activation de modules supplémentaires ou gestion d'une population d'utilisateurs supplémentaires sur le SI RH doivent se traduire par des évolutions idoines dans la solution IAM.

Evolutions des applications du périmètre

Si une application du périmètre migre vers le SaaS / Cloud ou monte en version, cela aura un impact sur la solution d'IAM mise en place. Des évolutions seront nécessaires, notamment pour adapter le provisioning de l'application ou encore pour transposer la solution de SSO.

Montées de version de la solution

L'éditeur de la solution propose des montées de version régulières pour corriger certaines limites de l'application, tenir compte des dernières préconisations de sécurité ou encore mettre à jour les composants de l'application. Un plan de montée de version doit être établi en prenant en compte qui fait quoi et à quelle fréquence. Le coût d'une telle action peut être évalué en avance de phase.

Migration d'OS

L'infrastructure du SI est également amenée à évoluer, partiellement ou plus largement. Cela peut poser de nombreuses questions : peut-on migrer le(s) serveur(s) sur le(s)quel(s) la solution est installée ? Comment la solution sera impactée par la migration d'OS ? Les flux inter-machines sont-ils maintenus ? Cela ne concerne pas forcément et uniquement les infrastructures serveur : dans le cas d'un projet eSSO par exemple, c'est la migration de l'OS des postes de travail qui peut avoir un impact sur la solution.

Incidents d'exploitation

Quelle que soit la qualité du travail réalisé pendant la phase projet, le risque d'un incident d'exploitation n'est jamais complètement écarté. Une fois le diagnostic posé sur l'origine de l'incident, il faut mettre en place les correctifs nécessaires à la solution. Généralement, cette brique de l'après-projet est relativement bien anticipée et traitée dans le cadre du MCO.

En synthèse

L'organisation du mode récurrent pose plusieurs questions. Lors de la phase projet, une équipe a été mise en place, généralement constituée d'internes et de prestataires, notamment d'intégrateurs.

Dans la phase d'après-projet, il faut définir les nouvelles responsabilités : quelle équipe en interne gère le mode récurrent ? Si ce n'est pas l'équipe projet, il faudra gérer le transfert de compétences. Quelles évolutions peuvent être gérées en interne ? Quelles évolutions nécessitent l'intervention d'experts de la solution ? Quels sont les rôles respectifs de l'intégrateur et de l'éditeur en mode récurrent ?

Dans l'idéal, le mode récurrent doit s'anticiper dès la phase projet. Il est en particulier fondamental d'envisager au plus tôt quels types de changements pourraient intervenir dans l'après-projet. Lors de la phase d'intégration, cela permet d'introduire de la souplesse dans la solution, là où on envisage des évolutions pour le futur. Parfois, si les changements envisageables sont importants, il peut même être utile d'intégrer ces questions dès la phase de sélection de la solution.

VII.2. Quel ROI pour un projet IAM ?

Quand une organisation se lance dans un projet de gestion des identités et des accès, ses objectifs sont généralement de sécuriser son système d'information ou d'améliorer l'expérience de ses collaborateurs. Le projet est vu comme une source de coûts, à mettre en balance face aux bénéfices attendus. Pourtant, un projet de gestion des identités et des accès permet également de réduire certains coûts de fonctionnement de l'entreprise et l'investissement initial peut être rentabilisé rapidement. Dans la suite de ce chapitre, nous allons présenter des éléments de réponse à la question : **quelles économies sont engendrées par un projet d'IAM et comment calculer le retour sur investissement (ROI) d'un tel projet ?**

VII.2.1. ROI d'un projet d'IAM

Le retour sur investissement est défini comme le rapport entre le bénéfice net du projet et l'investissement initial :

$$ROI = \frac{(Gains - Coûts\ d'investissement)}{Coûts\ d'investissement}$$

Note : il est également possible de chercher à estimer le temps de retour sur investissement, en amont d'un projet, qui va correspondre au temps nécessaire pour que les gains du projet soient supérieurs à l'investissement initial.

Dans le cadre d'un projet d'IAM, les coûts correspondent principalement :

- aux coûts d'achat des logiciels et aux coûts d'intégration, qui sont des coûts ponctuels au début du projet : phase de « BUILD » ;
- aux coûts annuels d'infrastructure et de maintenance du logiciel, et aux coûts de support et évolutions du projet : phase de « RUN ».

Du fait de l'automatisation de certains processus, il est légitime d'attendre d'un projet IAM la réalisation d'économies.

- Projet de gestion des identités - automatisation de la gestion des mouvements des utilisateurs du SI :
  - réduction du nombre d'actions manuelles à réaliser ;
  - réduction du nombre d'erreurs pendant le déroulement des différents processus.
- Projet de gestion des accès – authentification unique :
  - réduction du nombre de saisies manuelles des mots de passe ;
  - réduction du nombre de mots de passe à connaître, donc réduction du nombre de réinitialisations de mots de passe.

VII.2.2. L'automatisation de la gestion des arrivées / départs / mouvements

L'automatisation de la gestion des arrivées, départs et mouvements des collaborateurs permet de réduire le temps de traitement des demandes et donc de réduire les coûts de fonctionnement associés.

L'arrivée, la mutation et le départ d'un collaborateur nécessitent en effet un certain nombre d'opérations : par exemple son compte doit être créé, modifié, supprimé dans le logiciel central RH, dans l'annuaire ou les annuaires de l'entreprise. Sa boîte mail doit être créée ou supprimée, il faut lui donner ou supprimer des droits dans les applications de l'entreprise, etc.

Sans gestion d'identités, la plupart de ces actions doivent être réalisées manuellement. L'IAM vise à automatiser un maximum de ces actions. Dans une situation idéale, à l'arrivée d'un collaborateur, les ressources humaines créent toujours manuellement son compte dans leur logiciel RH, puis les comptes de l'utilisateur et ses droits sont gérés de façon automatique[(1)].

Les gains attendus par la mise en place d'un projet de gestion des identités vont ainsi dépendre du degré d'automatisation des processus, de la diminution du nombre d'actions à réaliser pour l'arrivée, le départ ou le mouvement d'un collaborateur, du temps moyen par action, du coût horaire du travail, mais aussi du nombre de procédures à réaliser, c'est à dire du turn-over, de la mobilité interne, de la politique de recours aux externes, ou encore de la croissance de l'entreprise.

En outre, chaque action manuelle représente un risque d'erreur. En automatisant les processus avec un projet de gestion des identités, le nombre d'actions manuelles à réaliser diminue, et par conséquent le nombre d'erreurs potentielles et les coûts qu'elles induisent.

Finalement, l'automatisation des procédures permet de réduire les délais d'obtention des habilitations pour les collaborateurs et donc d'améliorer leur productivité au moment d'une arrivée ou d'une mutation.

[(1)] Dans la pratique, il n'est pas rare de toujours avoir quelques actions manuelles à réaliser, pour certaines applications qui ne se prêtent pas au provisioning automatique pour des raisons techniques ou fonctionnelles. Il s'agit alors – pour les responsables du projet - de réaliser un arbitrage entre le coût de mise en place d'un provisioning automatique et le coût de conservation d'un provisioning manuel.

VII.2.3. L'authentification unique (SSO)

La mise en place d'une solution d'authentification unique permet de réduire le nombre de mots de passe qu'un utilisateur doit mémoriser, et donc de réduire le nombre de demandes de réinitialisations de mot de passe. Selon une étude de *Forrester ("Use Commercial IAM Solutions To Achieve More Than 100% ROI Over Manual Processes", by Andras cser, October 1, 2012),* un utilisateur oublierait en effet un mot de passe en moyenne quatre fois dans l'année. Or un mot de passe à réinitialiser représente non seulement des coûts pour le helpdesk en charge de la réinitialisation du mot de passe, mais également une perte de productivité pour le collaborateur en attente de son nouveau mot de passe.

L'authentification unique permet également de passer d'une situation où l'utilisateur doit saisir son login et son mot de passe dans chaque application, à une situation où il n'a à les saisir qu'une seule fois. Cela permettrait un gain de temps moyen par jour et par utilisateur de 9.51 minutes selon une étude de *Ponemon Institute (« How Single Sign-On Is Changing Healthcare - A Study of IT Practitioners in Acute Care Hospitals in the United States* » - *June 2011*)

VII.2.4. Bilan et limites du ROI

Quand une entreprise pense à mettre en œuvre un projet d'IAM, elle envisage les bénéfices qu'elle en retirera en termes de sécurité ou d'expérience d'utilisateur. Financièrement, elle estime le coût du projet en fonction de la solution choisie, en termes de coût de licences, de support et d'intégration. Mais elle omet généralement de tenir compte des gains financiers que le projet permettra de réaliser. Or, en tenant compte de ces gains, le temps de retour sur investissement apparaît beaucoup plus court. Selon les caractéristiques de l'entreprise, le projet sera potentiellement rentable dès les premières années suivant sa mise en place.

Mais le calcul du ROI présente certaines limites :

- D'un point de vue économique, les coûts et les bénéfices n'ont généralement pas lieu à la même période et il pourrait être intéressant d'actualiser les différentes valeurs. L'actualisation traduit la préférence pour le présent et l'aversion au risque. Pour en tenir compte, il est possible, par exemple de calculer la « Valeur Actuelle Nette » (VAN) du projet.

- Le ROI est un outil d'aide à la décision. Son calcul est réalisé en amont du projet, à partir d'estimations sur les gains - réduction du nombre d'appels au helpdesk, réduction du nombre d'actions manuelles à réaliser à l'arrivée d'un collaborateur - comme sur les coûts de licences et de jours d'intégration. Or il existe toujours un écart entre la solution envisagée et la solution mise en place : le nombre d'applications du périmètre peut évoluer, le temps d'intégration également, en fonction des difficultés rencontrées, des spécificités du projet et de l'environnement chez le client, etc.

- Peu d'organisations vont réellement connaître le coût que représente pour elles l'ensemble des actions manuelles à réaliser lors de l'arrivée d'un collaborateur ou lors d'un appel au helpdesk, sauf peut-être pour celles qui ont externalisé ce helpdesk. Ne connaissant pas le coût initial de ces opérations, elles ne seront peut-être pas sensibles à l'argument des gains réalisés sur ces postes.

- Peu de données sont disponibles sur les coûts que représentent les actions présentées ci-dessus. Les estimations peuvent varier fortement d'une source à l'autre. L'évaluation du ROI s'en trouve impactée et peut perdre en crédibilité pour certains. Il pourrait être intéressant de recueillir des données et de mettre en place des indicateurs pour estimer le temps de traitement d'une arrivée (gestion du cycle de vie des utilisateurs), la fréquence d'appels au helpdesk liés à des demandes de réinitialisation de mots de passe (self-service SSO), le nombre de saisies de mots de passe par jour et le temps passé (SSO), le nombre d'accès à telle ou telle application (contrôle d'accès), etc.

Enfin, il faut avoir à l'esprit que parler de ROI n'a de sens que si l'interlocuteur adressé y est sensible et que l'outil de ROI n'aura peut-être d'intérêt que si les éléments de gain, ou de « non–dépense », sont très précis sur, par exemple, l'économie réalisée sur les licences de telle ou telle application, la réduction des coûts de helpdesk dans le cas où ce service est externalisé, etc. De même, et au-delà de la productivité, n'oublions pas que les solutions d'IAM permettent également d'améliorer la sécurité, et donc de limiter des risques qui pourraient se matérialiser de manière financière.

VIII. Conclusion

Les membres du Groupe de Travail du CLUSIF ont souhaité apporter leur contribution au monde de l'IAM en fournissant, à travers ce document, une aide à la mise en œuvre de toute ou partie d'un projet de gestion et de gouvernance des identités et des accès.

Si le bien-fondé d'une démarche IAM est généralement admis, sa mise en œuvre n'en reste pas moins complexe. Ce document se veut ainsi un soutient dans cette démarche, posant les bonnes questions et apportant des axes de réponse.

Il a évidemment fallu faire des choix. C'est pourquoi nous avons fait celui de se concentrer sur les fondamentaux et ne pas traiter certains sujets techniques ou connexes.

Une fois ces fondamentaux mis en œuvre il sera probablement plus aisé d'aborder d'autres sujets, comme la gestion des identités et des accès des clients, ou celle des objets connectés.

"La pierre la plus solide d'un édifice est la plus basse de la fondation."

Khalil Gibran, poète, 1883-1931

IX. Annexes

IX.1. Glossaire

Le glossaire ci-dessous consiste à compléter le chapitre *« II. Principes fondamentaux de l'IAM et de l'IAG »*, et a vocation à fournir un éclairage sur un certain nombre de notions utilisées dans ce document.

Il peut également servir à initier un glossaire interne lors du lancement d'un projet IAM/IAG (cf. chapitre « *IV.3. Quelques conseils avant de commencer…* »).

Il ne fournit pas de définitions au sens académique ou littéraire, l'objectif étant plutôt d'expliquer de façon simple et pragmatique les termes utilisés dans ce document. Les explications fournies sont volontairement concises, le lecteur ayant tout loisir de se documenter plus en profondeur sur telle ou telle notion rapidement explicitée ici.

A noter également que ce glossaire contient uniquement des descriptions relatives à des termes utilisés dans l'IAM/IAG. Ceci afin de ne pas disposer d'un document trop volumineux. De même, nous n'avons pas redéfini des notions déjà expliquées dans le document, notamment toutes celles déjà définies au chapitre *« II. Principes fondamentaux de l'IAM et de l'IAG »*.

Les notions suivantes sont décrites :

Terminologie	Description
ABAC	*(Attribute-based access control)* Modélisation de droits d'accès dans laquelle les droits sont donnés par des attributs de la personne.
Accréditations (secondaires)	Pour une solution de eSSO, définit les couples login/mot de passe des utilisateurs qui seront joués par le moteur eSSO dans les fenêtres applicatives couvertes par la solution. Le terme « credential » est également utilisé.
Attribut	Représente une caractéristique d'un objet. Par exemple, une personne possède un nom et un prénom. Une organisation est caractérisée par un code, un nom d'affichage, une description, etc.
CAS	(*Central Authentication Service*) Désigne à la fois une solution et un protocole libres qui fournissent un service d'authentification unique Web.
Cercle de confiance	Dans le contexte de la fédération d'identités, définit un espace au sein duquel plusieurs fournisseurs (« fournisseurs d'identités » (IdP), « fournisseurs de services » (SP)) se seront accordés sur des règles de fonctionnement de la fédération d'identités.
Compte	Définition numérique d'une identité numérique sur un applicatif ou un système du SI. A ce compte sont souvent associés un authentifiant et un ensemble de droits et de données techniques. Il s'agit donc d'une notion technique. Il existe en général plusieurs types de comptes : compte utilisateur, compte de test, compte générique, compte de service, compte de formation, etc.
Compte dormant	Compte existant sur une application mais non utilisé par son propriétaire. Généralement, une règle de la politique IAM précise le critère définissant un compte dormant. Par exemple : tout compte associé à une identité et non utilisé depuis plus de 6 mois. Cette notion de « dormant » peut également être étendue à la notion de droit : un droit dormant est ainsi un droit possédé par un compte mais non utilisé par son propriétaire.
Compte de service	Compte utilisé sur un système afin de permettre l'exécution d'un processus ou d'une application. Un compte de service n'a pas vocation à être utilisé par un être humain à l'exception de certaines actions d'administration.
Compte orphelin	Compte qui n'est plus attaché à une identité de l'entreprise. Un compte orphelin peut résulter d'un processus d'habilitation non encore engagé ou de suppression de toutes ses habilitations.

Compte à privilèges	Compte disposant d'habilitations à-même de donner accès à des informations sensibles ou permettant de réaliser des opérations sensibles techniques et/ou fonctionnelles. Par exemple : compte administrateur, compte « root », opérateur de serveur, etc. Usuellement, cette notion fait référence aux comptes techniques, sur les composants d'infrastructure IT et exclut les comptes dans les applications ayant un très haut niveau d'autorisation, comme par exemple « SAP_ALL ».
Compte utilisateur	Compte attribué à tout utilisateur du SI. Par opposition au compte de service, un compte utilisateur est attribué à une personne.
Contrôle d'accès	Processus autorisant ou non l'accès à une ressource par un demandeur sur la base de son identification, son authentification et ses habilitations. Plusieurs niveaux de contrôle d'accès sont identifiables : • contrôle d'accès logique : accès oui/non à une application sans contrôle des droits ; • contrôle d'autorisation logique : contrôle plus fin, vérifiant que l'utilisateur dispose des droits nécessaires à l'action demandée ; • contrôle d'accès « physique » : aux bâtiments, aux parkings, à des salles sécurisées, etc. (aspect non traité dans ce document).
Délégation	Action qui consiste à confier une tâche à une (ou plusieurs) autre(s) personne(s) : le (ou les) délégué(s), sans pour autant que le délégant soit dégagé de sa responsabilité. En général une délégation est conditionnée par une date de début et une date de fin.
Droit	Correspond à une autorisation ou interdiction d'effectuer une action sur une ressource ou sur un élément d'une ressource. De manière usuelle, et sans définition stricte, un droit désigne généralement les autorisations les plus fines dans les applications. Un droit peut donc appartenir à plusieurs rôles ou profils applicatifs en général.
Droit exceptionnel	Droit accordé à un utilisateur en étant hors du modèle de droits. Les droits exceptionnels peuvent être accordés temporairement et être désactivés.
FIDO	*(Fast IDentity Online)* Alliance internationale d'organismes définissant des standards d'authentification forte.
Fournisseur d'Identités	(dans le contexte d'une fédération d'identités – cf. chapitre II.4.3.) Un fournisseur d'identités ou Identity Provider (IdP) : • garantit les moyens d'authentification des utilisateurs lors de l'accès à des services disponibles dans le cercle de confiance ;

	• transmet les informations d'identité telles que définies dans un accord initial ; • gère et supervise les accès sortants vers les ressources disponibles.
Fournisseur de services	(dans le contexte d'une fédération d'identités – cf. chapitre II.4.3.) Un fournisseur de service ou Service Provider (SP) : • met à disposition des ressources ou des services Web ; • valide les informations transmises par l'IdP et gère les identités fédérées : privilèges et autorisations, mises à jour d'attributs ; • assure la propagation des informations vers les services cibles ; • supervise les actions effectuées sur les services accédés.
Habilitation	Droit d'accès à une ressource.
Identité (numérique)	Représentation numérique d'une entité, physique ou morale, dans le référentiel de l'IAM, et plus largement sur le SI. En général, une identité numérique est constituée de : • un identifiant unique ; • l'ensemble des attributs qui caractérisent cette identité ; • l'ensemble des informations techniques nécessaires à la bonne utilisation de cette identité dans le monde numérique. Sauf cas exceptionnel, à une personne ou un objet correspond une seule identité, et à une identité correspond une seule personne ou objet.
Identifiant unique	Code unique permettant de référencer un objet de manière non ambiguë. Les bonnes pratiques précisent qu'un identifiant unique doit de plus être : • invariant dans le temps ; • non porteur d'information ; • sous une responsabilité ou une autorité unique, ou *a minima* sur un périmètre défini. Cet identifiant unique a comme utilité première d'être un identifiant de jointure, connu *a minima* de l'IAM. Idéalement, il est également renseigné dans un attribut de chaque compte de l'utilisateur. Par extension, et sans obligation, il peut également servir d'identifiant de connexion, c'est-à-dire de login.
Identification (processus d')	Processus de reconnaissance de l'identité d'une ressource.
LDAP	*(Lightweight Directory Access Protocol)*

	Désignait à l'origine un protocole d'interrogation d'annuaire. Par extension, un annuaire LDAP est un composant technique permettant de stocker des données de manière hiérarchique et normalisée.
Matricule RH	Il s'agit de l'identifiant au sens « RH » d'un employé dans le SI RH. Seuls les employés disposent ainsi de Matricule RH. Dans certains cas particuliers, une personne peut changer de matricule RH. C'est le cas lors d'une fusion de structures juridiques par exemple. Une personne peut également avoir plusieurs matricules RH lorsqu'elle possède plusieurs contrats de travail. Il est donc déconseillé d'utiliser le matricule RH, comme identifiant unique ou comme login, et ce même pour la population des employés. Néanmoins, les systèmes RH étant très souvent sources autoritaires pour les systèmes IAM, le matricule RH pourra être utilisé comme une clé de rapprochement entre IAM et SI RH.
Moindre privilège	Principe qui consiste à n'attribuer que les stricts privilèges nécessaires et pas davantage.
OAuth	Désigne un des standards utilisés dans la fédération d'identités.
Objet (IoT)	Définition numérique d'une entité non humaine dans un référentiel métier autoritaire, autre que le référentiel IAM, comme par exemple le référentiel véhicules.
OpenID Connect	Désigne un des standards utilisés dans la fédération d'identités.
OrBAC	*(Organization-Based Access Control)* Modélisation de droits d'accès dans laquelle les droits sont donnés par l'intermédiaire de rôles et par l'appartenance à une ou plusieurs organisations.
OTP	*(One-Time Password)* Mot de passe à usage unique, généré dynamiquement à partir d'une référence temporelle ou séquentielle, renouvelé après chaque authentification.
Permission	Droit fin sur une ressource, de type « lecture », « écriture », etc.
Personne	Définition numérique d'une entité humaine dans un référentiel métier autoritaire autre que le référentiel IAM, comme par exemple la base des ressources humaines pour les employés, la base clients, etc. La définition donnée dans l'ancien document du CLUSIF ne fait pas la distinction entre une « personne » et un « utilisateur du SI », ni entre une « personne » et une « identité ». Convenant qu'il faut laisser à la notion de personne un caractère humain et physique, il s'agit donc ici d'un individu. Considérant que derrière la personne morale il doit

	toujours y avoir au moins une personne physique, comme par exemple des fournisseurs ou des partenaires, la notion de personne morale ne s'applique pas dans le contexte de l'IAM. Elle est donc hors périmètre dans ce document.
Profil de connexion	Représente l'identité numérique et permet d'accéder au Système d'Information. Il est doté d'un identifiant unique qui peut servir de login. • à un profil de connexion correspond une seule identité numérique ; • à une identité numérique peuvent correspondre plusieurs profils de connexion ; • à chaque profil de connexion peuvent être attribués des rôles différents. Par exemple une identité peut avoir un profil de connexion standard pour les activités quotidiennes, et un profil de connexion de type administrateur pour les activités plus sensibles.
RBAC	*(Role-Based Access Control)* Modélisation de droits d'accès dans laquelle les droits sont donnés par l'intermédiaire de rôles.
Recertification (processus de)	Processus qui vise à revalider ou reconfirmer une information. Il existe plusieurs processus de recertifications : • recertification d'équipe, visant à confirmer les liens entre les managers et leurs subordonnés ; • recertification des prestataires, visant à confirmer la présence des prestataires ; • recertification des habilitations, visant à confirmer la pertinence des habilitations attribuées. Les recertifications sont généralement menées sous forme de campagnes, avec une ouverture, une période de revue et une clôture. Ces campagnes peuvent être ponctuelles ou conduites à intervalles réguliers.
Réconciliation	Opération consistant à lire des informations, telles que des comptes ou des droits, sur une ressource, et à les rapprocher des informations dans le système IAM, telles que des identités ou des habilitations.
Ressource	Partie matérielle ou logicielle d'un système informatique pouvant être employée par différents utilisateurs. Elle correspond à la typologie de cible : la ressource est généralement logicielle (AD, SAP, Google, etc.) mais elle peut également être matérielle (moyen d'authentification, téléphone, badge d'accès, etc.).

Rôle (ou profil) applicatif	Correspond à un regroupement de droits pour une même application généralement. Un rôle (ou profil) applicatif possède un ensemble d'attributs précisant la définition du rôle applicatif. Un contexte peut être défini pour préciser la portée du rôle, comme par exemple un périmètre, une période de validité. Un rôle applicatif est souvent attribué à des profils de connexion, et un rôle applicatif peut appartenir à plusieurs rôles (ou profils) métiers.
Rôle (ou profil) métier	Correspond à un regroupement de rôles applicatifs. Un rôle métier possède un ensemble d'attributs précisant la définition du rôle. Un contexte peut être défini pour préciser la portée du rôle, comme par exemple un périmètre, une période de validité.
SAML	*(Security Assertion Markup Language)* Désigne un des standards utilisés dans la fédération d'identités.
SoD	*(Segregation Of Duty)* La SoD ou « Séparation Des Tâches » permet de préciser l'incompatibilité de rôles entre eux. Il peut y avoir plusieurs niveaux d'incompatibilité entre eux, comme par exemple : • la demande de deux rôles incompatibles n'est pas possible : soit ils ne sont pas visibles ensemble, soit la demande entraîne un refus automatique d'affectation ; • la demande de deux rôles incompatibles déclenche un processus de validation particulier ; • la demande de deux rôles incompatibles est autorisée mais elle est annotée comme nécessitant une surveillance particulière, telle qu'une recertification à fréquence régulière.
WS-Federation	Désigne un des standards utilisés dans la fédération d'identités.

IX.2. Fiche « Cahier des charges IAM »

Cette annexe vient compléter la question « Q7 : Quels sont les éléments à ne pas oublier dans mon cahier des charges ? » et propose un exemple de « sommaire type » d'un cahier des charges possible. L'idée étant d'insister ici sur toutes les sections à développer.

1. Introduction
    a. Objet du document
    b. Contexte du document
    c. Enjeux du projet
2. Existant
    a. Organisation et processus
    b. SI
        i. Utilisateurs et usages
        ii. Infrastructures
        iii. Applications
3. Besoins
    a. Exigences fonctionnelles
        i. Gestion des identités
        ii. Gestion des habilitations
        iii. Authentification
        iv. SSO
        v. Contrôle d'accès
    b. Exigences techniques
        i. Sécurité
        ii. Infrastructure
        iii. Qualité de service
    c. Architecture fonctionnelle cible
    d. Contraintes / Spécificités du contexte
4. Fournitures attendues
    a. Prestations
    b. Outillage
    c. Livrables
    d. Planning
5. Modalités de réponse

IX.3. Fiches techniques SSO

Les éléments ci-après peuvent être utilisés lors la phase de cadrage et de préparation d'un projet de SSO, ou pendant les ateliers de spécifications. Ils permettent d'identifier toutes les informations nécessaires à l'intégration des applications dans le projet et facilitent cette dernière lors de la phase de réalisation. Il faudra, idéalement, remplir, faire remplir, ou se faire aider à remplir, une fiche par application. Les informations n'étant pas les mêmes selon la nature du projet (eSSO / WebSSO / Fédération d'Identités), ces fiches traitent de généralités puis de particularités propres à chacun de ces modes de SSO.

IX.3.1. Généralités

Question	Réponse
Nom / référence de l'application	
Description de l'application	
Editeur de l'application + contacts	
Date de création de la fiche	
Date de modification de la fiche	
Auteur de la fiche	
Type d'application (Client Lourd/ Client léger/ Web)	
Niveau de disponibilité ?	
Existe-t-il de la documentation technique pour cette application ?	
Disponibilité d'un environnement de tests pour cette application ?	
Disponibilité de comptes de tests pour cette application ?	

IX.3.2. Questions spécifiques au eSSO (entreprise SSO)

Question	Réponse
Type d'application : • Windows • DotNet ou Accessible ou Console • Web (+ navigateurs utilisés) • AS400/ehllapi (Emulateur) • Java • Autre ?	
Type de fenêtre à enrôler : • Authentification • Erreur d'authentification • Changement de mot de passe • Erreur de changement de mot de passe	

• Autre ?	
Attributs à gérer (+type) : • Login (syntaxe « texte simple ») • Password (syntaxe « password ») • Autres : domaine, email, rôle, (type liste, boolean, …)	
L'application a-t-elle une politique de mot de passe particulière ? Celle-ci doit-elle être surchargée par la solution eSSO ?	
Le référentiel utilisateur de l'application est-il identique au référentiel principal (ex AD, LDAP Primaire) ? Sinon quel est-il ?	
Les utilisateurs peuvent-ils avoir plusieurs comptes sur l'application (multi-compte : utilisateur, administrateur, …) ?	
L'application intègre-t-elle une interface de changement de mot de passe ?	
L'application doit-elle être exécutée de manière automatique à l'arrivée de l'utilisateur ?	
L'application doit-elle être interrompue lors d'un changement d'utilisateur ? (cas du mode « kiosque » ou « partagé ») Dispose-t-elle d'un « changement rapide utilisateur » ?	
L'application peut-elle être exécutée plusieurs fois dans une même session Windows ? (cas du mode « multi-bureau »)	
L'utilisateur peut-il lancer l'application depuis le client eSSO ?	
L'application nécessite-t-elle une réauthentification primaire ? (application sensible) Avec quelle méthode d'authentification ?	
L'accès à l'exécution de l'application doit-il être protégé ? Est-ce que la solution eSSO doit bloquer le lancement de l'application si l'utilisateur n'est pas autorisé à l'utiliser ?	
Les utilisateurs peuvent-ils déléguer leur compte applicatif ?	
Certains utilisateurs ont-ils des comptes partagés sur l'application ?	
L'utilisateur peut-il se déconnecter ? (auquel cas la solution ne doit pas réauthentifier automatiquement l'utilisateur)	
L'application est-elle intégrée à la solution interne de gestion des habilitations ? Si oui, les accréditations de l'application sont-elles provisionnées de manière automatique vers la solution de eSSO ?	

IX.3.3. Questions spécifiques au WebSSO et à la fédération d'identités

En WebSSO, l'approche est en général plus complexe et nécessite souvent une analyse plus poussée des applications à intégrer par des experts SSO, intégrateurs ou éditeurs. Les spécifications doivent permettre de définir les grandes tendances, à savoir s'il est possible de faire de la fédération d'identités, et laquelle, s'il est possible d'utiliser des méthodes de SSO via API, Web Service ou valve applicative, ou si le sujet est abordé par d'autres méthodes de SSO Web : entêtes HTTP, remplissage de formulaire, réécriture d'URL, etc. Le choix de la méthode de SSO à appliquer est donc très dépendant de l'application et certaines questions ne sont pas du ressort du responsable de l'application, mais plutôt du responsable du projet SSO, voire d'autres responsables techniques d'annuaires LDAP, AD, etc.

Question	Réponse
Informations techniques	
Plateforme serveur (OS)	
Serveur Web (type/version/options)	
Technologie applicative (ASP, JSP, …)	
Criticité d'accès (sécurisation forte ?)	
Niveau de disponibilité mis en place au niveau du serveur	
Protocole d'accès à l'application ? (HTTP / HTTPS)	
Emplacement réseau de l'application ? (Intranet, DMZ, SaaS…)	
Est-il possible d'installer un agent sur le serveur applicatif ? (Module Apache, Filtre ISAPI, Valve Tomcat…)	
Les utilisateurs accèdent-ils à l'application via un Reverse Proxy ? Si oui, est-il possible d'installer un Agent SSO sur le Reverse Proxy ?	
Cinématiques utilisateurs	
Quelles sont les cinématiques d'accès à l'application ? • Lien dans un portail ? • Liens dans des mails ? • Favoris ?	
Ces liens sont-ils toujours fixes (ex. : page d'accueil de l'application) ou peuvent-ils être dynamiques (ex. : page avec un identifiant de dossier) ?	
Comment l'utilisateur s'authentifie-t-il dans l'application actuellement ?	
Doit-on conserver un accès possible à l'application sans passer par le SSO ?	
Quelle est l'URL saisie par les utilisateurs pour accéder à l'application ? (à détailler par environnement : production, pré-production, etc.)	

Méthode de SSO	
Quels sont les mécanismes d'authentification (ou de SSO) supportés par l'application ? • Formulaire HTML • Basic HTTP • Header HTTP • Kerberos / NTML • SAMLv2 • OAuth2 / OpenID Connect • Certificat X509 • Autres ?	
L'application est-elle modifiable ? (notamment : l'authentification de l'application peut-elle être surchargée ?)	
Cas particulier : application compatible SAMLv2	
Nom du partenaire de fédération / Contacts	
Technologie utilisée par le partenaire (ADFS, OpenSSO, OpenSAML, etc.) ?	
Version du protocole SAML à utiliser (1.1, 2.0) ?	
Rôle assuré par la solution interne dans cette Fédération : • IdP : fournisseur d'identités • SP : fournisseur de service / consommateur d'identités	
Quel est l'initiateur de la séquence de Fédération (mode « IdP Initiated » ou « SP Initiated »)	
SAML Profiles	
SAML Binding	
Les assertions SAML doivent-elles être signées ?	
Les demandes d'authentification (AuthNRequest) doivent-elles être signées ?	
Mode de Fédération (Temporaire ou Permanent)	
Nom de l'attribut SAML portant l'identité de l'utilisateur (si fédération temporaire seulement)	
Identifiant utilisateur	
Attributs nécessaires (lister les attributs envoyés par l'IdP ou nécessaires au SP)	
Autres informations ?	

IX.4. Annexe « authentification forte »

L'objectif de cette annexe est de fournir quelques éléments relatifs aux différentes technologies d'authentification, simple ou forte, déployées sur le marché. Afin d'aider le lecteur qui serait en phase de sélection d'une telle technologie à arbitrer en fonction de ses contraintes, nous proposons quelques avantages et inconvénients des différents choix possibles.

En préambule, rappelons que le chapitre « II.3. Authentifier les utilisateurs » de ce document présente les grands concepts de l'authentification.

IX.4.1. Identification simple

Identifiant + Mot de passe	*Avantages*	• Facile à mettre en œuvre
	Inconvénients	• Nécessite une politique de mot de passe complexe • Les mots de passe peuvent être craqués, par force brute par exemple • Gestion des oublis des mots de passe
	Ergonomie	• Gestion de mots de passe multiples • Notation des identifiants sur post-it • « Irritant » pour l'utilisateur
	Sécurité	• Faible
	Coût	• Moyen
RFID	*Avantages*	• Facile à déployer • Pas de mot de passe à retenir • Supports RFID variés
	Inconvénients	• Nécessite des lecteurs RFID • Sécurité de la transaction carte-lecteur faible • Risque de perte/vol/casse du support
	Ergonomie	• Pas de code PIN pour sécuriser l'accès au support • Support multi-services : couplage avec le contrôle d'accès physique par exemple
	Sécurité	• Faible
	Coût	• Faible

IX.4.2. Authentification forte à 2 facteurs

RFID/Mot de passe	*Avantages*	• Pas de gestion de certificats • Pas d'usure, longévité du support • Supports RFID variés : clé USB, smartphones, cartes, etc. • Personnalisation graphique possible
	Inconvénients	• Nécessite des lecteurs de carte RFID • Sécurité de la transaction carte-lecteur faible • Risque de perte et vol du support • Pas de code PIN pour sécuriser l'accès au support
	Ergonomie	• Support multi-service • Facilité d'utilisation, mode sans-contact • Identification rapide du personnel
	Sécurité	• Moyenne
	Coût	• Faible
Carte à puce + code PIN	*Avantages*	• Sécurité : nécessite un code PIN pour autoriser l'accès à la carte • Usage des certificats : signature, chiffrement, authentification • Pas de mot de passe à gérer • Vol : pas d'accès direct au certificat en raison de la protection par code PIN • Personnalisation graphique possible
	Inconvénients	• Risque de perte ou d'oubli du support • Nécessite un lecteur de carte contact et le déploiement d'un middleware • Nécessite de gérer des certificats : PKI, CMS, etc.
	Ergonomie	• Support fiable, robuste • Facilité d'utilisation • Identification rapide du personnel • Support multi-services possible grâce au RFID
	Sécurité	• Elevée
	Coût	• Elevé
Token USB + code PIN	*Avantages*	• Sécurité : nécessite un code PIN pour autoriser l'accès au token • Usage des certificats : signature, chiffrement, authentification • Pas de mots de passe à gérer • Vol : pas d'accès direct au certificat en raison de la protection par code PIN • Pas besoin de lecteur de carte • Stockage de données possible

	Inconvénients	• Risque de perte ou d'oubli du support • Nécessite de gérer des certificats • Nécessite l'accès aux ports USB
	Ergonomie	• Support fiable, robuste • Facilité d'utilisation • Support multi-service possible grâce au RFID • Stockage de fichiers personnels chiffrés
	Sécurité	• Elevée
	Coût	• Elevé
Biométrie (Match on Card)	*Avantages*	• Sécurité : ce que je suis • Conformité CNIL « Match On Card », contrairement au mode « Match On Server » notamment
	Inconvénients	• Prix élevé • Lecteurs spécifiques
	Ergonomie	• Nécessite d'enrôler les empreintes • Pas de mot de passe à retenir
	Sécurité	• Elevée
	Coût	• Elevé

IX.4.3. Authentification forte à 2 facteurs [Hors Bande]

OTP SMS	*Avantages*	• Rien à installer • Facilité d'utilisation avec la recopie d'un code par exemple • Rien à retenir
	Inconvénients	• Coût de la plateforme d'envoi de SMS • Nécessite d'avoir son téléphone sur soi • Nécessite d'avoir accès au réseau GSM • Le numéro de téléphone des utilisateurs doit être connu
	Ergonomie	• Très facile d'accès: compatible avec tous types de téléphones • Usage classique, courant tel que paiement 3DSecure par exemple
	Sécurité	• Moyenne
	Coût	• Elevé
OTP Mail	*Avantages*	• Rien à installer • Facilité d'utilisation avec la recopie d'un code par exemple • Rien à retenir

	Inconvénients	• Nécessite d'avoir un téléphone mobile connecté au réseau • Nécessite une adresse mail • Faiblesse de la sécurité du mail : interception
	Ergonomie	• Usage classique des téléphones mobiles
	Sécurité	• Moyenne
	Coût	• Moyen
OTP Smartphone (PUSH)	*Avantages*	• Sécurisation de l'application de génération du code OTP par mot de passe ou PIN • Fonctionne en mode déconnecté c'est-à-dire hors réseau
	Inconvénients	• Nécessite une application sur le smartphone • L'enrôlement du périphérique doit avoir été effectué au préalable
	Ergonomie	• Facile à installer sur un smartphone professionnel
	Sécurité	• Elevée
	Coût	• Moyen
Jetons Electroniques / soft token	*Avantages*	• Jeton d'authentification unique
	Inconvénients	• Nécessite une infrastructure serveur • Risque de perte ou vol
	Ergonomie	• Nécessite d'avoir le jeton sur soi
	Sécurité	• Moyenne
	Coût	• Moyen

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr