www.evidian.com

L'IAM : un outil stratégique pour répondre aux exigences des marchés financiers

Sommaire

« Extension sécurisée de votre SI au-delà des frontières classiques »

« Synopsis d'une banque multinationale »

Le cas étudié ici est celui d'une banque composée de quelques milliers d'employés situés dans plusieurs dizaines de pays dans le monde. Son projet consiste à proposer ses services de gestion de fonds de manière sécurisée à ses clients, filiales et partenaires. L'ouverture de l'accès au système d'information constitue un axe majeur du développement de l'entreprise et engendre diverses problématiques de sécurité et de gestion du cycle de vie des utilisateurs.

Création, modification et suppression d'un nouveau client ou partenaire, génération des droits d'accès aux diverses applications qui lui seront attribuées tout au long de son contrat, disponibilité des personnes validant les autorisations, traçabilité de bout en bout des actions effectuées,... sont autant d'exigences requises lors du déploiement d'un tel projet.

En plus de la problématique évoquée, il faut également tenir compte du personnel opérant au sein de l'entreprise : ces personnes disposent souvent de droits d'accès excessifs par rapport à leurs rôles et constituent un vecteur des défaillances de sécurité.

Afin de répondre aux exigences réglementaires, les acteurs des marchés financiers et de l'assurance doivent mettre en place des dispositifs pour maîtriser leurs risques opérationnels. Ces obligations se traduisent notamment par la mise en place de mécanismes pour renforcer le contrôle des accès au système d'information, dans le but de protéger l'intégrité et la confidentialité des données.

En parallèle, face à l'augmentation du nombre d'applications informatiques – et donc du nombre de mots de passe à retenir – ces entreprises cherchent des solutions sécurisées pour augmenter la productivité de leurs collaborateurs et alléger le travail des services d'assistance à l'utilisateur. Ces solutions doivent aussi permettre la mise en place de méthodes d'authentification forte afin de garantir une sécurité maximale. Aussi, il est impératif de disposer d'une solution intégrée et évolutive afin de ne pénaliser ni les utilisateurs finaux, ni les services d'administration et d'exploitation de ces solutions.

Régulièrement présente au cœur de l'actualité économique, la gestion des identités et des accès est devenue un enjeu majeur de la gouvernance des entreprises du secteur financier.

Chronologie d'une gestion des identités et des accès

Suite aux évolutions techniques récentes, les marchés financiers se retrouvent avec plus d'opportunités pour développer leurs activités. L'irruption du monde « Web », du « cloud » et des multiples moyens d'accès à l'information permet aux entreprises de mettre en place des processus métier et des activités allant au-delà des frontières classiques des environnements techniques.

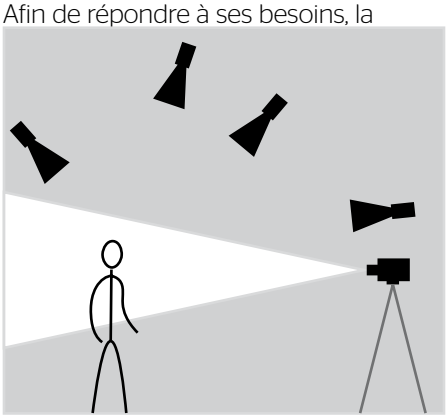
Les problèmes qu'une banque peut rencontrer sont les mêmes que peuvent rencontrer une compagnie d'assurance, un groupement hospitalier ou une institution regroupant les professionnels d'un secteur d'activité. Ces organisations peuvent aujourd'hui mettre en place des solutions centralisées, mutualisées, accessibles par leurs différents établissements, filiales ou partenaires.

Néanmoins, elles ont tout de même besoin d'être rassurées sur la sécurité, la facilité et la traçabilité des accès aux services offerts sans pour autant voir se démultiplier la charge d'administration. Il est impératif qu'elles puissent déléguer cette administration des utilisateurs locaux à des responsables intermédiaires ou directement aux utilisateurs finaux en leur permettant de faire leurs propres demandes. Des processus de délégation ou de validation peuvent être nécessaires pour s'assurer du bien-fondé des demandes.

Il est aussi important de pouvoir réutiliser les infrastructures déjà en place sans avoir à modifier celles existantes, comme par exemple le site web.

Considérons le cas d'une banque souhaitant étendre son système d'information afin d'offrir à ses clients et filiales une gestion fine et sécurisée des identités et des accès.

Afin de répondre à ses besoins, la



solution envisagée devra :

- Offrir un système de demande de création de compte,
- Sécuriser l'accès aux comptes récemment créés moyennant un système d'activation limité dans le temps et permettant à l'utilisateur final de définir son mot de passe en conformité avec la politique de sécurité interne,
- Disposer d'un système d'assignation des droits des utilisateurs basé sur les besoins liés au métier de chaque utilisateur en s'assurant que l'utilisateur a uniquement les droits nécessaires à son métier et pas plus. Ceci, par exemple, dans le but d'isoler « front office, middle office et back office »,
- Permettre aux « métiers », c'est-à-dire aux responsables proches des utilisateurs, de faire des demandes de droits pour eux ou de valider/refuser les demandes faites par leurs collaborateurs,
- Pouvoir facilement déléguer des tâches d'administration liées au cycle de vie des utilisateurs à des cellules spécifiques,
- Proposer un panel d'authentifications fortes adaptées à la sensibilité des actions effectuées,
- Permettre à l'utilisateur de ne retenir aucun mot de passe supplémentaire pour réaliser son travail sans mettre en péril la sécurité de l'entreprise,
- Pouvoir continuer à utiliser le portail web existant de l'entreprise sans avoir à le modifier pour offrir les fonctionnalités décrites précédemment,
- Disposer d'outils de reporting et de traçabilité avancés afin de permettre la gouvernance et la conformité à la réglementation en cas d'audit.

Il est évident que les points mentionnés ne constituent pas la liste exhaustive des fonctionnalités qu'une banque exigera de la solution de gestion des identités et des accès qu'elle doit implémenter, mais ceux-ci donnent un aperçu assez représentatif du cœur du problème.

Dans les sections suivantes, ce livre blanc présente ce qu'Evidian propose pour aider à résoudre ces problématiques.

La proposition d'Evidian :

La proposition d'Evidian est basée sur sa Suite Identity and Access Management (IAM). La Suite IAM d'Evidian permet de répondre positivement aux besoins exprimés précédemment et d'aller au-delà des points indiqués, notamment en matière de gouvernance des accès et de gestion des identités.

La Suite IAM d'Evidian est un ensemble de produits développés entièrement par Evidian et nativement intégrés, couvrant l'ensemble fonctionnel présenté dans la figure ci-dessus.

La capacité à définir une politique de gouvernance des accès et des identités constitue le cœur de la Suite IAM d'Evidian. Elle permet de gérer qui peut accéder à quelles applications, avec quels droits, à partir d'où et comment.

Elle amène aussi des fonctionnalités permettant de :

- vérifier, à tout moment, que cette politique est respectée,
- simuler les impacts d'un changement de politique.

La Suite IAM d'Evidian facilite la constitution d'un annuaire d'identités incluant toutes les personnes accédant au système d'information en provenance de différentes sources d'identités. On retrouvera dans cet annuaire aussi bien les employés que les externes ou les partenaires. C'est sur cet annuaire d'identités que la politique de gouvernance des accès et des identités s'appliquera.

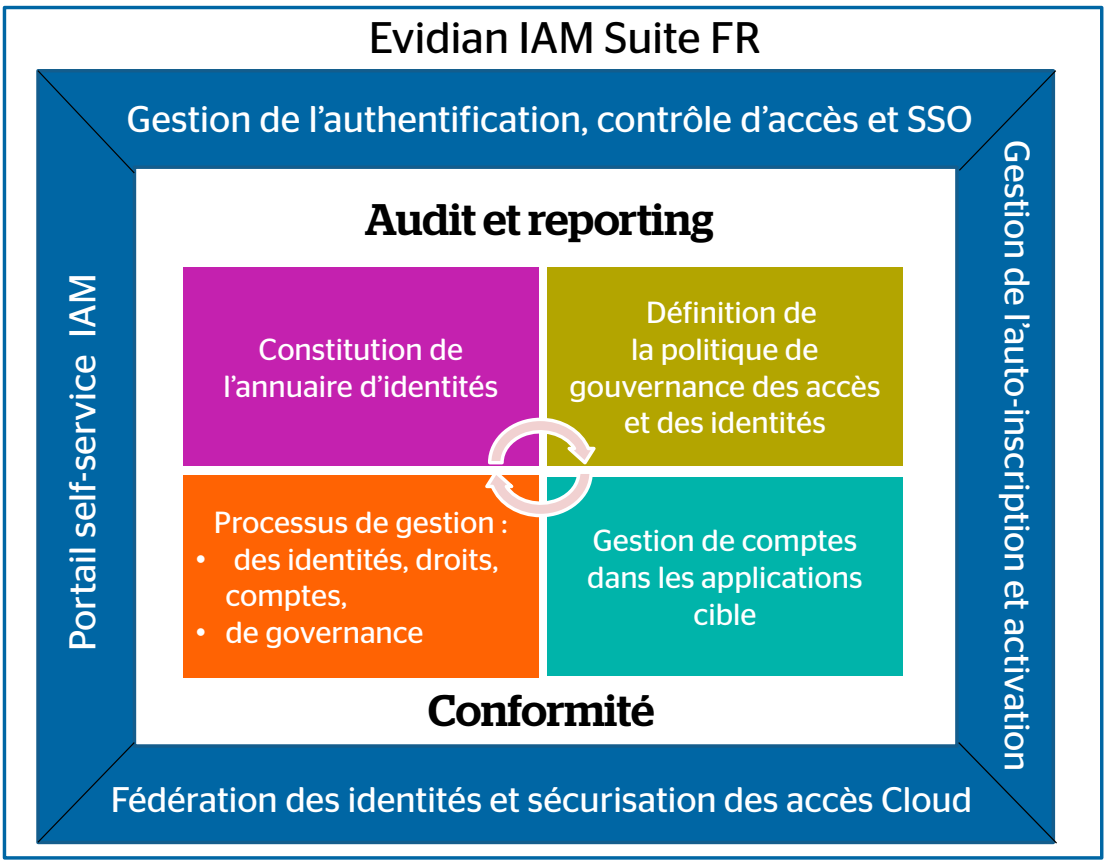
Les différents processus proposés, en standard, par la Suite IAM d'Evidian, permettent à l'entreprise de donner à ses utilisateurs le moyen de réaliser, entre autres, leurs demandes de droits, consulter l'annuaire d'identités, tenir à jour leurs propres données d'identité et déclarer l'arrivée ou le départ d'une personne. Ceci s'effectue de façon structurée en impliquant les bonnes personnes dans les actions d'approbation ou réalisations associées.

Ils permettent aussi de réaliser un suivi des actions en cours. Ces processus sont disponibles sur le portail IAM pour les utilisateurs finaux.

En fin de processus d'attribution de droits, la gestion des comptes dans les applications cibles permet d'appliquer la politique de gouvernance des accès et des identités.

Les fonctions d'authentification, de contrôle d'accès et de SSO sécurisent et facilitent l'accès à tous types d'applications. Elles sont complétées par les fonctions de fédération d'identités et de sécurisation d'accès aux applications dans le Cloud, afin de fournir un environnement de travail homogène à l'utilisateur final.

Bien entendu, toutes les actions réalisées sont auditées et il est possible d'obtenir des rapports, aussi bien des actions d'administration que des accès des utilisateurs au système d'information.



Modéliser les besoins en droits d'accès

Afin de pouvoir assigner des droits d'accès aux utilisateurs, la Suite IAM propose d'utiliser un modèle de droits basé sur les modèles RBAC et OrBAC. Ces modèles permettent d'associer des droits à un rôle. Ce rôle représente normalement un métier dans l'entreprise. Afin d'éviter la prolifération de rôles, Evidian utilise aussi la notion d'organisation pour définir les droits des personnes qui exercent un métier dans une organisation donnée.

Il est également possible d'assigner des droits de façon directe sans passer par l'assignation d'un rôle afin de traiter les exceptions.

Le modèle apporte également des notions d'inclusions organisationnelle et hiérarchique ou d'exclusion afin de faciliter la tâche de l'assignation des droits associés à un rôle et sa gestion. Les règles de séparation de pouvoirs permettent de s'assurer de la cohérence en évitant d'assigner des droits antinomiques à une même personne.

Cette modélisation des droits va aussi être utilisée dynamiquement en interne pour identifier les acteurs et leurs droits lors de l'exécution des processus proposés par la Suite IAM.

Par exemple, on donnera à un manager le rôle de « valideur des demandes de droits ». Pour pouvoir optimiser davantage la solution, il nous reste à délimiter la portée du droit. Cette capacité est fournie par l'utilisation de la notion de contexte. Ainsi, un contexte peut être « les personnes de mon équipe », « les personnes de tel agence », « les externes », etc. C'est ainsi que différents circuits d'habilitation peuvent être modélisés et exploités en fonction de plusieurs critères.

Cette notion de contexte peut aussi s'appliquer à d'autres objets. Par exemple, pour déterminer la liste d'applications proposées à un employé lorsqu'il réalise une demande de droits, on peut limiter les informations affichées dans les pages blanches ou bien limiter les informations modifiables dans les interfaces de processus de workflow livrés avec la Suite IAM.

L'utilisation de ces notions rend la solution très flexible et puissante : elle s'adapte aux besoins changeants de l'entreprise. Tout est paramétrable, réduisant ainsi les coûts d'opération.

Faciliter l'assignation des droits et suivre les évolutions

Une fois la modélisation des droits réalisée, il est important de pouvoir facilement assigner ces droits aux employés mais aussi d'avoir des mécanismes permettant de suivre les évolutions fonctionnelles des employés, avec les changements en termes de droits associés.

La Suite IAM d'Evidian propose d'utiliser les valeurs d'attributs des utilisateurs pour leur assigner des rôles qui vont impliquer des droits. Cette attribution de droits se fait sur l'application de règles, nommées règles métier. Elles permettent de définir les rôles à associer à des personnes en fonction des valeurs de certains attributs de ces personnes. Il est aussi possible de définir des exceptions. Par exemple, toutes les personnes travaillant dans une agence doivent avoir le rôle « Accéder à l'application déclaration des congés », sauf les externes.

Cette fonction permet très facilement d'assigner un ou plusieurs rôles à un nouvel arrivant mais aussi d'adapter dynamiquement les nouveaux rôles qu'un employé obtiendra lors de sa mutation au sein de l'entreprise. Un employé d'une filiale qui vient d'être intégrée au siège obtient automatiquement les droits nécessaires à son nouveau métier.

Bien entendu, il est possible de conserver, pendant un certain temps, l'ensemble des droits associés à sa filiale et ceux du siège pour faciliter la période de transition entre les deux postes.

L'utilisation des règles métier n'est pas le seul moyen d'assigner des rôles à des personnes. Il est aussi possible de le faire en utilisant les processus d'assignation de rôle.

Déléguer la responsabilité aux métiers

La Suite IAM d'Evidian propose en standard une série de processus pour la gestion des identités, des rôles et des droits, des comptes et des services. A titre d'exemple, nous pouvons citer : déclaration d'un nouvel employé, départ d'un employé, mutation dans une autre organisation, demande de droits pour soi-même ou une autre personne, modification des attributs d'un compte, déclaration d'une période de longue absence, création de dossiers partagés, etc. Actuellement plus de 40 processus sont livrés en standard.

En utilisant ces processus, les décisions dans l'assignation de droits et la gestion du cycle de vie des utilisateurs sont complètement déléguées aux métiers. On passe d'une administration centralisée à une administration au plus proche « du terrain »

Assurer à tout moment la conformité des droits

La Suite IAM d'Evidian fournit les processus et fonctionnalités nécessaires pour réaliser les contrôles concernant les droits des employés. Les processus de certification de droits permettent aux managers de valider/corriger les droits actuels d'un seul ou d'un ensemble de collaborateurs.

Des fonctions, comme la réconciliation, permettent de détecter des écarts entre ce qui a été défini comme étant les droits qu'un employé doit avoir et les droits qu'il a en réalité. Des actions correctives sont ensuite proposées pour permettre à l'entreprise de réagir et ajuster cet écart.

Réutiliser l'infrastructure existante

La Suite IAM d'Evidian peut s'intégrer dans l'environnement existant sans demander de modification. A titre d'exemple, l'image ci-après présente le site Web d'Evidian, sécurisé par la Suite IAM, qui assure une authentification et dont la structure n'a pas été changée. Cela permet aux utilisateurs authentifiés de bénéficier de services avancés. Le formulaire d'authentification et les liens vers les services sécurisés sont ajoutés sans modification du site existant..

Possibilité de demander un compte et sécuriser son activation

La Suite IAM d'Evidian offre un mécanisme d'auto-activation et la possibilité de demander un compte d'accès.

Dans le cas présent, la personne peut indiquer l'agence où elle travaille, son métier et une adresse mail par exemple. En utilisant ces données, les demandes seront envoyées aux bonnes personnes et les bons droits lui seront assignés.

La Suite IAM permet ensuite deux modes de fonctionnement :

- soit les identifiants/mots de passe sont communiqués par SMS et/ou mail.
- soit la personne doit activer son compte et choisir le mot de passe qu'elle utilisera à l'avenir pour se connecter au système d'information.

S'authentifier avec son téléphone

La Suite IAM d'Evidian permet à un employé de s'authentifier avec un QR Code via son smartphone.

Les utilisateurs peuvent s'authentifier avec d'autres méthodes comme :

- L'identifiant et le mot de passe,
- Le clavier virtuel qui permet à un utilisateur de fournir son identifiant et son mot de passe en cliquant sur un clavier positionné aléatoirement à l'écran. Ce clavier virtuel offre une protection supplémentaire contre les « key loggers » sans nécessiter de périphérique ou de logiciel supplémentaire,
- OTP (One Time Password ou mot de passe à usage unique),
- Carte à puce avec certificat X .509,
- Jeton SAML (Service Provider/ Identity Provider),
- Méthode d'authentification à base du protocole Radius,
- « Grid Card password », chaque utilisateur dispose d'une carte individuelle permettant de résoudre un challenge non rejouable,
- SMS OTP ou Mail OTP, chaque utilisateur a la capacité de disposer d'un OTP via son téléphone portable et/ou sa messagerie,
- Kerberos et les authentifications de domaine Windows,
- Des mécanismes d'authentification externes comme CAS, OpenID, OAuth ou le couplage avec n'importe quel mécanisme externe en utilisant le SDK.

Zéro mot de passe à retenir

La Suite IAM d'Evidian offre la fonctionnalité d'authentification unique (SSO) et de fédération d'identités.

L'employé s'authentifie une fois et ensuite, toute nouvelle demande d'authentification pour accéder à une application hébergée dans la banque ou dans le Cloud est prise en compte par la Suite IAM.

Adieu les problèmes de perte de mémoire après un long weekend ou des vacances !

Conclusion

Grâce à la mise en place de la Suite IAM d'Evidian, une banque pourra mettre à la disposition de ses clients, partenaires et filiales, une solution de gestion des identités et des accès permettant, entre autres, de :

Gérer les identités des personnes accédant au système d'information,

Déléguer la gestion des droits aux interlocuteurs les plus proches connaissant les besoins métiers de ces personnes,

S'assurer que la politique de gouvernance des accès mise en place est respectée à tout moment,

Permettre de prendre en compte immédiatement les changements des droits des personnes : mutation, évolution contractuelle, etc .

Evoluer avec les changements d'organisation de l'entreprise,

Donner aux employés l'autonomie pour gérer les accès sans mettre en péril la sécurité de l'entreprise,

Offrir un accès simple et sécurisé sans mots de passe à mémoriser,

S'adapter à l'infrastructure .

Sans être exhaustif dans la description des capacités de la Suite IAM d'Evidian, ce livre blanc montre qu'Evidian est le partenaire idéal pour aider les acteurs des marchés financiers à répondre à leurs problématiques.

La Suite IAM d'Evidian

Notre solution IAM est reconnue par les clients et les analystes pour sa complétude. En effet, elle offre les composants suivants, pouvant être déployés indépendamment ou intégrés nativement :

- Evidian Identity & Access Manager

  permet la gouvernance des autorisations et une gestion complète du cycle de vie des identités et des accès aux services, pilotée par une politique de sécurité et ses workflows d'approbation.

- Evidian Web Access Manager

  fédère des accès aux applications web, sécurise l'accès des utilisateurs mobiles et remplace l'ensemble des mots de passe des utilisateurs par un mode d'authentification forte et unique.

- Evidian Enterprise SSO

  gère l'accès aux applications d'entreprise et personnelles sur les postes de travail ainsi que sur les terminaux mobiles, libère l'utilisateur de mémoriser et saisir les mots de passe.

- Evidian Authentication Manager

  offre l'authentification forte sur les postes de travail et terminaux mobiles : carte ou token avec certificat, carte sans contact, biométrie, mot de passe à usage unique.

- Evidian SafeKit

  apporte la haute disponibilité et le partage de charge aux applications.