Evidian

L'IAM pour une entreprise étendue

Trusted partner for your **Digital Journey**

Sommaire

04 “Une entreprise de la grande distribution”

05 L’évolution de la gestion des identités et des accès

06 La proposition faite à Franck

06 Modéliser les besoins en droits d’accès

07 Faciliter l’assignation des droits et suivre les évolutions

07 Déléguer la responsabilité aux métiers

08 Assurer à tout moment la conformité des droits

08 Réutiliser l’infrastructure existante

08 Possibilité de demander un compte et sécuriser son activation

09 S’authentifier avec son téléphone

09 Zéro mot de passe à retenir

10 Conclusion

10 La Suite IAM d’Evidian

Etendez le SI de votre entreprise au-delà des frontières classiques de façon sécurisée

“Une entreprise de la grande distribution”

Franck, directeur informatique et Cathy, directrice marketing du groupe, un lundi matin, à la machine à café.

Cathy: Bonjour Franck, comment vas-tu ?

Frank: Bof, hier nous avons perdu à la dernière minute à cause d’un penalty inexistant, tu te rends compte ?

Cathy: Oh-la-la, toi et le foot ! Mais rassure-moi ce n’est pas pour pour ça que tu fais cette tête, non ? Je t’offre un café ?

Frank: Merci, avec plaisir. Non ce n’est pas pour ça que je fais cette tête. Vendredi dernier Benjamin, le Directeur Financer, m’a convoqué car nous devons mettre en place un système permettant d’identifier, dans chaque magasin, qui se connecte au système de commandes. Les comptes génériques par magasin ne peuvent plus être utilisés.

Cathy: Bon, tu exagères, ça ne doit pas être si compliqué, non ?

Frank: Tu plaisantes sans doute ? Avec les nombreux mouvements de personnel que nous avons dans nos 80 magasins dans toute l’Europe, il est impossible pour moi de savoir qui doit accéder à quoi. C’est pour cela que nous avions mis en place les comptes génériques.

Cathy: En fait, il n’y a que le responsable du magasin qui peut le savoir, non ?

Frank: Exactement ! Comme on dit, il n’y a que les managers ou les responsables d’une activité qui peuvent savoir qui doit accéder à quoi et avec quels droits.

Cathy: Pourquoi, tous les commerciaux n’ont pas les mêmes droits ?

Frank: Ah non, non, en fonction de leur niveau de responsabilité ou du rayon où ils travaillent, les droits peuvent être différents. En plus pour certaines applications, le responsable du magasin peut donner directement un accès, par contre pour d’autres, il faut que la demande soit validée en central et devine…

Cathy: Devine quoi ?

Frank: Pour faire simple, celui qui peut valider en central une demande de droits d’un responsable magasin pour un commercial n’est pas toujours le même.

Cathy: Cela commence à devenir compliqué ton affaire ! Parce qu’en plus, maintenant que j’y pense, tous les magasins n’ont pas de responsable attitré n’est-ce pas ?

Frank: Voilà, il va falloir permettre aux commerciaux de faire leurs propres demandes d’accès ou même de s’auto-inscrire s’ils ne sont pas encore définis dans le système. Tu sais, pour la paie, il suffit que la personne soit dans le système avant la dernière semaine du mois, mais nous, mous avons besoin de préparer son environnement de travail plusieurs jours avant son arrivée afin qu’elle puisse travailler tout de suite.

Cathy: Et elle devra elle-même “activer” son compte dans un délai court, pour garantir un minimum de sécurité…

Frank: Bien vu Cathy !

Cathy: En plus, tu vas faire face aux nouvelles exigences de tous les usagers, ils vont te dire qu’ils doivent pouvoir se connecter avec leur téléphone, et sans mot de passe. On oublie tout après un long weekend !

Frank: Et pas question de modifier quoique ce soit dans le site web. il vient juste d’être validé par la direction et il est accepté par tous les utilisateurs aussi bien les internes que les externes.

Cathy: Ah oui au fait… vous pouvez encore être champions ou bien c’est fini ?

Frank: Non, c’est fini. Bon, allez, je te laisse il faut que je trouve une solution miraculeuse à tous ces problèmes. A plus.

Cathy: A plus, bon courage et si tu as besoin d’aide…

Franck, notre directeur informatique doit permettre à son entreprise de respecter les réglementations. De plus il doit prendre en compte les nouvelles évolutions technologiques récentes. Voyons maintenant en termes de solution informatique et fonctionnelle comment l’aider dans cette démarche.

L'évolution de la gestion des identités et des accès

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

Les problèmes que Franck rencontre dans son entreprise de distribution sont les mêmes que peuvent rencontrer une entité financière internationale, 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 quand même le 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 validation sont nécessaires pour s'assurer du bien-fondé des demandes.

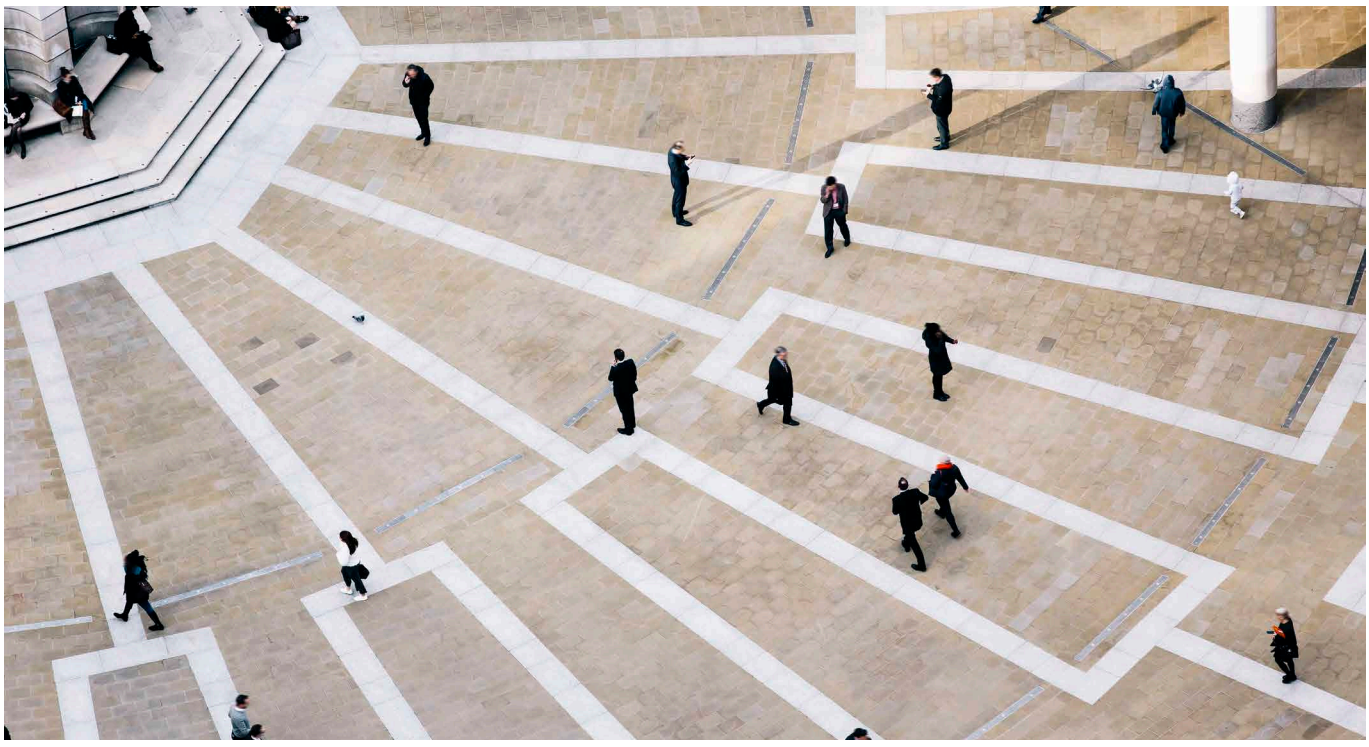
Il est aussi important de pouvoir réutiliser les infrastructures déjà en place sans avoir à modifier l'existant, comme par exemple le site web.

En analysant la discussion entre Franck et Cathy, on s'aperçoit que l'entreprise a besoin de :

- Pouvoir assigner des comptes uniques à chaque utilisateur au lieu d'utiliser des comptes génériques, ceci afin d'assurer audit et traçabilité des accès,
- Disposer d'un système d'assignation des droits des utilisateurs basé sur les besoins liés au métier de chaque utilisateur avec des éléments de contrôle pour s'assurer que l'utilisateur a uniquement les droits nécessaires à son métier et pas plus,
- 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. Bien entendu il faut que le choix proposé aux utilisateurs, lors de la demande de droits, soit adapté à leur métier et que les demandes de validation soient envoyées aux bonnes personnes,
- Offrir un système de demande de « création de compte » aux employés qui n'ont pas encore été définis dans le système d'information pour permettre l'accès au système d'information de façon contrôlée,
- Sécuriser l'accès aux comptes récemment créés moyennant un système d'activation, avec une durée de vie limitée dans le temps, permettant à l'utilisateur final de définir son mot de passe en conformité avec une politique de mot de passe,
- Permettre, si l'utilisateur le souhaite, de s'authentifier avec son téléphone ou tablette et n'avoir à retenir aucun mot de passe pour réaliser son travail sans mettre en péril la sécurité de l'entreprise,
- Et finalement, pouvoir continuer à utiliser le portail web existant sans avoir à le modifier pour offrir les fonctionnalités décrites précédemment.

Il est évident que les points mentionnés ne constituent pas la liste exhaustive des fonctionnalités que Franck demandera à la solution de gestion des identités et des accès qu'il doit implémenter mais donnent un aperçu assez représentatif du coeur du problème.

Dans les sections suivantes ce livre blanc présente ce qu'Evidian peut proposer à Franck pour l'aider à résoudre son problème.



La proposition faite à Franck

La proposition faite à Franck est basée sur la suite Evidian Identity and Access Management (IAM). La Suite Evidian IAM lui 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 Evidian IAM est un ensemble de produits développés entièrement par Evidian et nativement intégrés, couvrant l'ensemble fonctionnel présenté dans la figure ci-dessous.

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

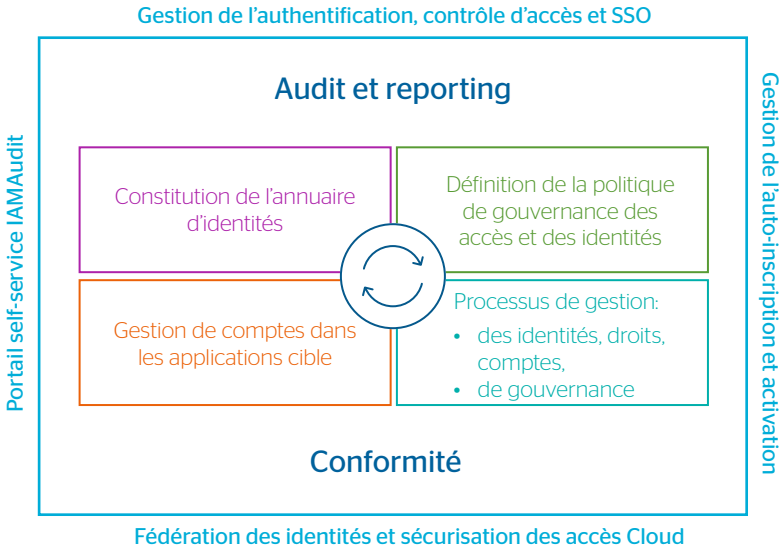
Elle amène aussi des fonctionnalités permettant de :

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

Les différents processus proposés, en standard, par la Suite Evidian IAM, 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, ou déclarer l'arrivée ou le départ d'un personne. Ceci s'effectuant 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.

Evidian IAM Suite



Les fonctions d'authentification, contrôle d'accès et SSO permettent de sécuriser et faciliter 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.

Dans les sections suivantes nous présentons les avantages que la Suite Evidian IAM apportera à Franck et son entreprise.

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[1] et OrBAC[2]. 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.

A titre d'exemple, tous les managers de rayon ont un minimum de droits communs mais aussi d'autres droits en fonction du rayon (HIFI, boissons...) dans lequel ils travaillent.

1 - RBAC : Role Based Access Control
2 - OrBAC : Organisation Based Access Control

Il est aussi possible, bien entendu, d'assigner des droits de façon directe sans passer par l'assignation d'un rôle car il faut pouvoir traiter les cas qui n'ont pas pu être modélisés ou les exceptions.

Le modèle apporte également des notions d'inclusion organisationnelle et hiérarchique, d'exclusion et de règles de séparation de pouvoirs. Ces notions ont pour objectifs, d'une part de faciliter la tâche de l'assignation des droits associés à un rôle et sa gestion, et d'autre part de s'assurer de la cohérence 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 de rayon le rôle de « valideur des demandes de droits ». Ensuite on indiquera, dans le processus de demande de droits, que celle-ci doit être validée par une personne ayant le rôle « valideur des demandes de droits ». Pour pouvoir optimiser d'avantage la solution, il nous reste à pouvoir 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 magasin », « les externes », etc. En appliquant ce contexte au droit « valider une demande de droits », seules les demandes de droits des personnes de mon équipe, ou d'un magasin ou des externes me seront envoyées.

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, 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, rendent la solution très flexible et puissante pour s'adapter aux besoins changeant 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 réalisé, 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 un magasin 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 magasinier qui devient responsable d'entrepôt 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 au magasinier et au responsable d'entrepôt 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 Evidian IAM propose en standard une série de processus pour la gestion des identités, des rôles et 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 soit même ou une autre personne, modification des attributs d'un compte, déclaration d'un 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 », peu importe où il se trouve.

La proposition faite à Franck

Assurer à tout moment la conformité des droits

La Suite Evidian IAM 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 collaborateur ou d'un ensemble de collaborateurs.

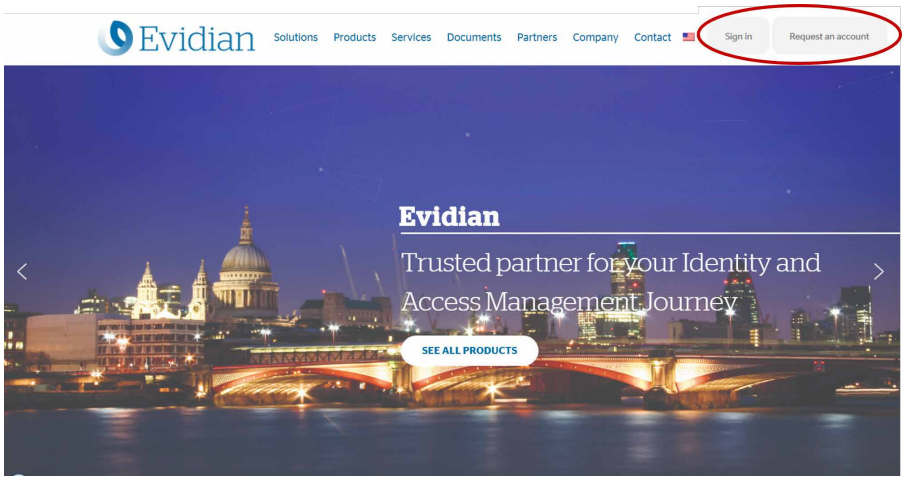
Des fonctions, comme la réconciliation, permettent de détecter des écarts entre ce qui a été défini comme étant les droits qu'un employé doit avoir et les droits qu'il a en réalité. Des actions correctives sont ensuite proposées pour permettre à l'entreprise de réagir et ajuster cet écart.

Réutiliser l'infrastructure existante

La Suite Evidian IAM peut s'intégrer dans l'environnement existant sans demander de modifications[3].

Franck a indiqué la création d'un nouveau site Web et précisé qu'il était hors de question de le modifier pour intégrer les nouvelles fonctionnalités demandées. Ceci est tout à fait possible avec la Suite Evidian IAM.

A titre d'exemple, l'image ci-dessus présente le site Web d'Evidian sécurisé par la Suite IAM qui assure une authentification (encadré en rouge). 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 Evidian IAM offre la possibilité de demander un compte d'accès.

Dans le cas présent la personne peut indiquer le magasin où elle travaille, son métier et une adresse mail, par exemple. En utilisant ces données, les mécanismes présentés précédemment permettent de s'assurer que les demandes seront envoyées aux bonnes personnes et que les bons droits lui seront assignés.

La Suite IAM permet ensuite deux modes de fonctionnement :

- Soit les identifiants/mots de passes sont communiqués par SMS et/ou mail,
- Soit la personne reçoit un mail avec un lien paramétrable, d'une durée de vie limitée, lui demandant d'activer le compte qui vient de lui être créé. A ce moment l'utilisateur pourra choisir le mot de passe qu'il utilisera à l'avenir pour se connecter au système d'information.

Une fois le compte activé, la personne pourra accéder de manière sécurisée aux applications autorisées.

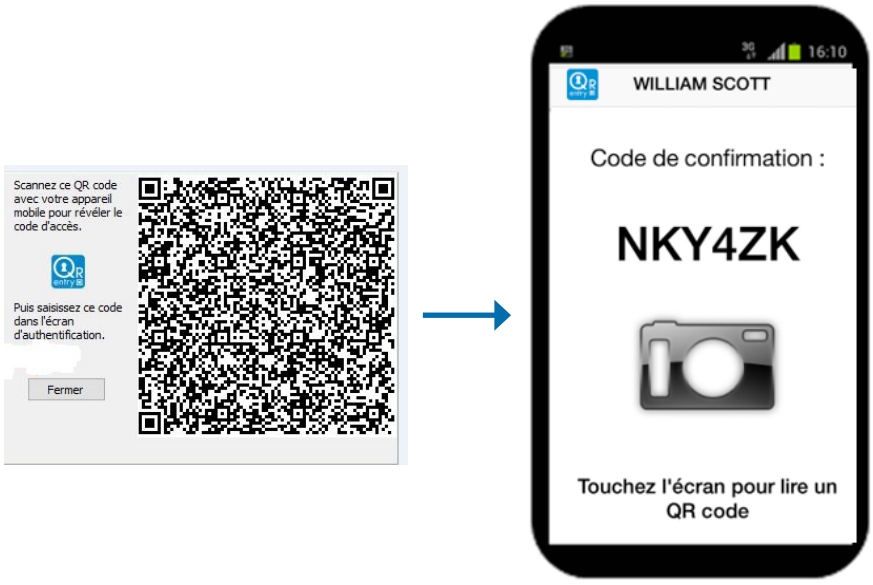
3 - Il est néanmoins rappelé que les environnements techniques sur lesquels peuvent être installés les produits logiciels Evidian doivent répondre aux prérequis techniques indiqués dans la documentation.

S'authentifier avec son téléphone

La Suite Evidian IAM permet à un employé de s'authentifier avec un QR Code via son smartphone. Pour ce faire, il faut qu'au préalable l'employé « déclare » son smartphone à l'entreprise. Cette « déclaration » se fait au travers de la Suite IAM par l'employé lui-même, sans l'intervention du département informatique.

La Suite IAM peut authentifier les utilisateurs avec d'autres méthodes comme :

- L'identifiant et le mot de passe,
- Le clavier virtuel. Ce clavier virtuel 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,
- Social login, services d'authentification des réseaux sociaux (LinkedIn, Twitter...),
- « Grid Card password », chaque utilisateur dispose d'une carte individuelle permettant de résoudre un challenge non re-jouable,
- SMS OTP ou Mail OTP, chaque utilisateur à 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 un SDK.



Zéro mot de passe à retenir

La Suite Evidian IAM offre la fonctionnalité d'authentification unique (SSO). Avec cette fonctionnalité, l'employé s'authentifie une fois et ensuite toute nouvelle demande d'authentification pour accéder à une application est prise en compte par la Suite IAM.

De ce fait, si l'on prend le cas d'un employé qui utilise son smartphone pour s'authentifier sur le portail de l'entreprise, la Suite IAM d'Evidian permet à Franck d'annoncer qu'il a mis en place une solution sécurisée avec zéro mot de passe à retenir.

Adieu au problème de perte de mémoire après un long weekend ou de retour de vacances !

Conclusion

Grâce à la mise en place de la Suite Evidian IAM, Franck pourra mettre à la disposition de sa société une solution de gestion des identités et des accès permettant, entre autre, 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, longues absences, 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 Evidian IAM, ce livre blanc montre qu'Evidian est le partenaire idéal pour aider Franck à répondre aux demandes de sa société.

La Suite Evidian IAM

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 unique et forte.

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.

Pour plus d'information, visitez notre site web : **www.evidian.fr**

* Règlement Général sur la Protection des Données

Prérequis au RGPD*

La gouvernance des accès est un élément parmi l'ensemble de mesures techniques permettant de mitiger les risques liés à le protection des données. En plus de ses fonctionnalités de revue et de certification de droits, Evidian IGA prend en compte les obligations du droit à la personne. Des fonctionnalités en libre service et des rapports dédiées permettent l'exercice des droits utilisateurs et des processus conforme au RGPD.

Brochure

À propos d'Evidian

Evidian est la suite logicielle de gestion des identités et des accès (IAM), d'Eviden.

Evidian IAM est le leader européen des logi ciels de gestion des identités et des accès, avec une présence en pleine croissance en dehors du continent européen et notamment aux Etats-Unis et au Japon.

Plus de 5.000.000 d'utilisateurs dans plus de 900 organisations dans le monde entier se connectent tous les jours à leur entreprise et gèrent leurs droits d'accès avec les solutions de gestion des identités et des accès d'Evi dian.

© Eviden. Evidian est une marque déposée, propriété d'Eviden. Tous les produits, noms, marques et autres éléments, cités dans ce document appartiennent à leurs propriétaires respectifs et peuvent être protégés au titre des lois et règlements régissant la propriété intellectuelle.
Evidian se réserve le droit de modifier les caractéristiques de ses produits sans avis préalable.

CT_J1269_180803_RY_B_LAIMPOURLEN