Evidian

Méthodes d'authentification forte multifacteurs (MFA) Quel choix pour le poste de travail en entreprise ?

Trusted partner for your **Digital Journey**

Introduction

Ce livre blanc présente les méthodes d'authentification forte les plus utilisées dans les organisations, avec leurs spécificités.

Il détaille les problèmes les plus fréquemment rencontrés dans les phases de déploiement et d'administration quotidienne. Il présente les solutions couramment mises en œuvre.

Les techniques d'authentification fortes en entreprise sont fréquement imposées par les réglementations. De plus en plus d'organisations les utilisent pour protéger les accès internes et externes.

Mais dans la pratique, les déploiements d'authentification forte sont souvent plus longs et coûteux que prévu. La faute en est rarement à la technologie elle-même, mais plutôt à la façon dont elle est mise en œuvre :

- Cas d'usage imprévus : kiosque en libre service, accès à plusieurs postes simultanément, délégation, mobilité, terminaux légers...
- Gestion des oublis de cartes et les approvisionnements.
- Utilisateurs (souvent influents) aux besoins particuliers.
- Support des équipements de nombreux différents fournisseurs.

Par conséquent, il faut anticiper les coûts cachés d'un déploiement d'authentification forte, sous peine de manquer de budget et de main d'œuvre après quelques semaines. Cela dit, de bons choix initiaux peuvent largement éviter les déconvenues.

Ce document se base sur plus de 20 ans d'expérience de déploiements d'authentification dans des organisations (de 500 à 200 000 utilisateurs). Il présente les techniques d'authentification et leurs limites, puis offre des conseils pratiques pour le déploiement et la gestion de l'authentification forte.

Authentification forte : les bases

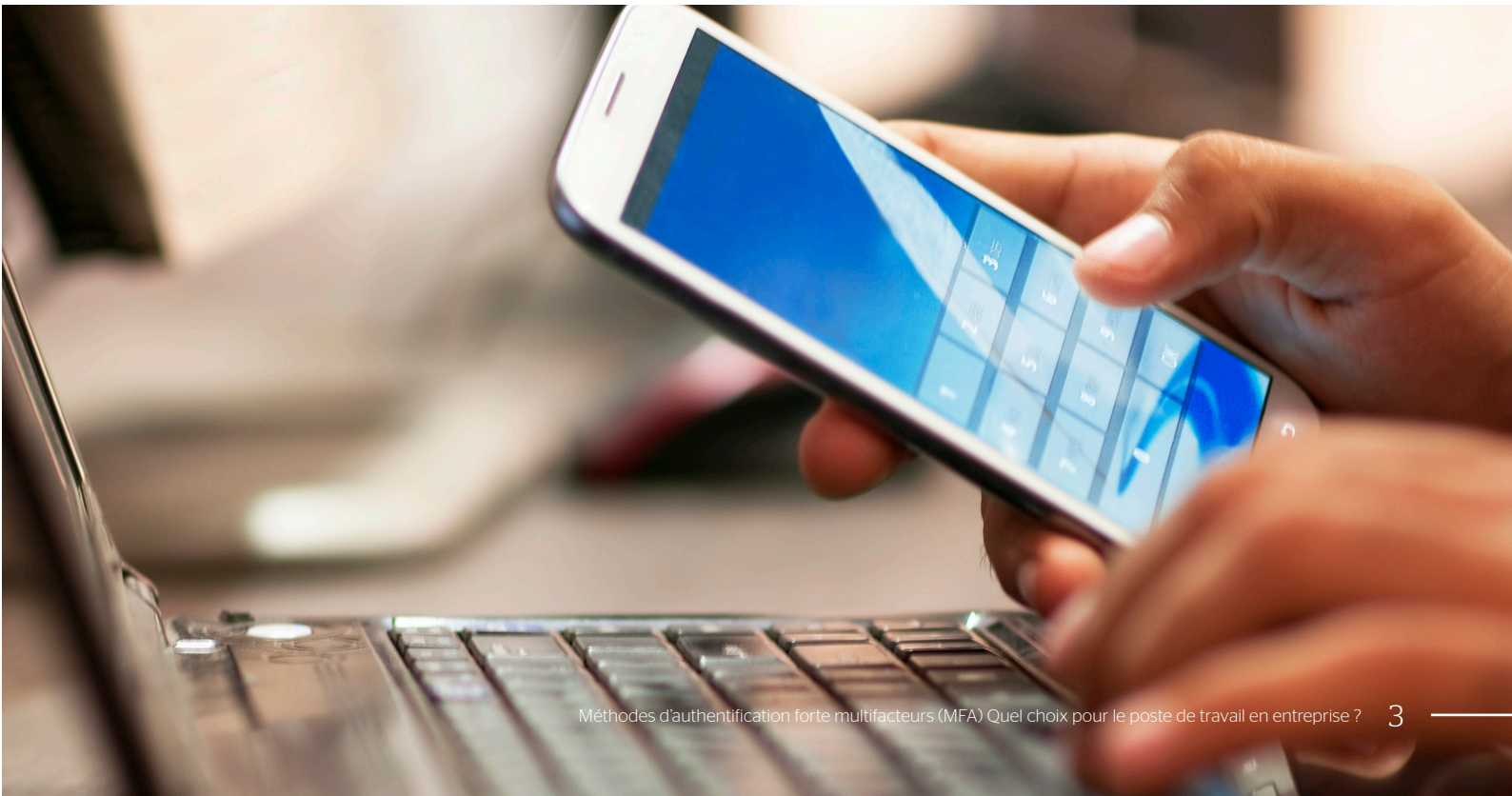
Bien utilisée, l'authentification forte permet de renforcer le contrôle d'accès au système d'information. Un utilisateur déclare qui il est (identification) puis prouve son identité (authentification) – en renforçant ces deux étapes, vous rendez votre activité plus sûre :

Intégrité : Évitez que des informations importantes ne soient modifiées	Données comptables et financières, résultats d'analyse…
Confidentialité : Seules les personnes autorisées consultent les informations	Dossier médical, numéros de carte de crédit…
Disponibilité : Le bon fonctionnement de l'entreprise n'est pas altéré	Comptes d'administrateur, gestion de production…
Audit : Évitez que les auteurs d'actions nient les avoir commises, enquêtez sur un incident	Stations de traders dans une banque, vente en magasin…
Business: Augmentez le sentiment de sûreté chez vos clients	Vente en ligne, sous-traitance de la défense nationale

Toutes les fonctions de l'entreprise n'ont pas la même criticité. Il peut être envisageable d'équiper de cartes à puce uniquement les vendeurs des magasins ou le personnel soignant d'un hôpital – le reste de l'organisation se contentant alors d'utiliser des mots de passe. Autre exemple, seules les applications servant à la chaîne de tests d'une entreprise pharmaceutique nécessitent une authentification biométrique.

Au démarrage d'un projet, il est donc nécessaire d'en préciser clairement les objectifs. Ceux-ci seront exprimés de façon fonctionnelle, voire 'business' et non techniques. Validée par les parties prenantes, cette « charte » servira de ligne directrice lors du déroulement du projet :

- Périmètre : utilisateurs, organisations, ressources…
- Objectifs principaux : intégrité, confidentialité, disponibilité, audit…
- Contraintes : besoins spécifiques, profils critiques, délais.



Les 7 méthodes d'authentification les plus utilisées

Un utilisateur fournit en général deux éléments pour accéder à une ressource protégée :

- Un élément (nom, numéro dans l'annuaire etc.) qui permet son **identification**.
- Un ou plusieurs éléments permettant d'assurer **l'authentification**.

Un utilisateur peut prouver son identité par ce qu'il connaît (identifiant/mot de passe), ce qu'il possède (carte à puce, badge RFID) ou ce qu'il est (biométrie). Voici les méthodes d'authentification qu'Evidian rencontre le plus souvent dans les organisations :

Type d'authentification	Description
1. Mot de passe	Simple, voire rustique, son plus gros défaut est que le niveau de sécurité dépend directement de la complexité du mot de passe. La conséquence : des mots de passes trop complexes et nombreux poussent les utilisateurs à utiliser des contournements : Post-It™, fichier Excel ou liste dans un smartphone. **Identifiant et mot de passe sont la méthode d'authentification la plus utilisée. Des solutions d'authentification unique (SSO) peuvent pallier à la multiplication de mots de passe.**
2. Mot de passe à usage unique ('one-time password' - OTP)	L'OTP permet d'éviter qu'un mot de passe ne soit volé et réutilisé. Un système OTP fournit un mot de passe à la demande. Ce mot de passe est valide pendant une durée limitée, et pour une seule utilisation. **L'OTP est en général utilisé pour l'authentification initiale à des accès externes via VPN. Il ne nécessite aucune configuration de la station ou du Smartphone d'accueil. Il est aussi utilisé comme complément à l'authentification par mot de passe pour offrir une authentification multifacteur (MFA).**
3. Certificats sur carte à puce	Les certificats sont utilisés pour chiffrer ou signer des messages sans avoir à partager de secret. L'identifiant est un certificat public qui est signé et donc garanti par une autorité de certification reconnue. L'utilisateur doit fournir un élément secret - le code PIN de sa carte - pour pouvoir utiliser les différents éléments cryptographiques. **Cette solution est souvent utilisée pour l'authentification initiale ou l'accès aux applications web ou de messagerie. Elle nécessite une infrastructure à clé publique (PKI).**
4. Smartphone – OTP – notification Push	Le smartphone peut être un moyen d'authentification. Les méthodes suivantes sont principalement utilisées : • Lors de l'authentification, un mot de passe à usage unique est envoyé par SMS ou par par email, • Lors de l'authentification, une notification Push est présentée à l'utilisateur sur son smartphone, • Une application installée sur un smartphone calcule elle-même un mot de passe à usage unique. • Une application scanne un QRcode qui contient un OTP chiffré (ex. : EvidianQRentry). **Le smartphone est souvent utilisé en cas d'oubli du mot de passe ou de la carte à puce, notamment lors des accès depuis internet.**

Type d'authentification	Description
5. Biométrie	L'authentification par biométrie vérifie le plus souvent l'empreinte digitale ou veineuse de l'utilisateur. Les données biométriques de l'utilisateur sont stockées sur un serveur central (avec des contraintes légales fortes), sur le poste ou sur une carte à puce. **La biométrie est en général mise en œuvre pour l'authentification initiale ou pour protéger l'accès à des applications très sensibles.**
6. Badge sans contact	Une puce insérée dans un badge porte un code qui identifie un utilisateur. Il s'agit donc au sens propre d'une identification qui, couplée à un mot de passe ou à un PIN, peut être utilisée dans des procédures d'authentification. Le plus souvent, la techonologie utilisée est du RFID passif (HID, MIFARE...), la carte ne possède pas d'alimentation propre. Elle est alimentée lors de la lecture par un champ électromagnétique généré par le lecteur. Le badge doit être rapidement présenté au dispositif pour ouvrir la session Windows ; celle-ci se verrouille lorsque le badge est représenté puis retiré. **Le RFID passif est souvent utilisé pour le contrôle d'accès physique par badge ou le paiement au restaurant d'entreprise. La détection d'une carte de ce type se fait à quelques centimètres.Cette technologie est souvent combinée avec des cartes à puce pour s'assurer que l'utilisateur retire sa carte du lecteur puisque qu'il aura besoin de la partie sans contact pour accéder au batiment ou s'offrir un café** Vous pouvez également utiliser la technologie du RFID actif, cependant le badge doit être alimenté par une pile, ce qui vous contraint donc de gérer un stock de piles et d'anticiper leur fin de vie. Le badge doit être placé à proximité du dispositif, pour ouvrir la session Windows ; celle-ci est verrouillée lorsque le badge est retiré.
7. Objet connecté (Wearable)	Un équipement bluetooth généralement de type bracelet offre un moyen d'authentification sans fil testé dans les centres d'innovations des entreprises. Selon le niveau de sécurité de l'équipement, le bracelet peut servir d'identifiant ou d'authentifiant si le bracelet demande une authentification pour être activée. **Cette technologie est utile pour réaliser de l'authentification continue. La technologie bluetooth permet de garantir la présence de l'utilisateur à proximité du poste de travail. Lorsque le signal est trop faible le poste se verrouille.**

Coût et ergonomie des méthodes d'authentification

Type d'authentification	PC + hardware	PC only	Smartphone	Cost	Usability
1. Mot de passe	✓	✓	✓	•	••
2. OTP	✓	✓	✓	••	•
3. Push Notification	✓	✓	✓	•	•••
4. Certificats PKI sur carte	✓			••	••
5. Smartphone	✓	✓	✓	••	•
6. Biométrie	✓			••	•••
7. Badge sans contact	✓			••	••
8. Objet connecté (wearable)	✓			•••	•••

Combiner les méthodes d'authentification

D'autres technologies existent. Ainsi, il est possible d'exiger qu'une authentification s'effectue uniquement sur un nombre limité d'équipements. Une station de travail sera alors identifiée par son adresse réseau ou ses caractéristiques matérielles uniques. Dans la pratique, de nombreuses combinaisons sont rencontrées, par exemple :

- Certaines ressources exigent plusieurs éléments d'authentification : empreinte digitale et carte à puce, par exemple. On parle alors d'authentification à plusieurs facteurs.
- A l'opposée, une organisation peut estimer qu'une simple identification suffit : par exemple, en présentant un badge sans contact pour accéder à un site.

Bieen sûr, il faut arbitrer les besoins en terme de sécurité ou de facilité d'utilisation. Une solution très sûre pourra être rejetée par des opérationnels si elle leur impose trop de contraintes. On dit alors que « trop de sécurité tue la sécurité ».

Etude de cas

Dans les hôpitaux, le soin aux patients est prioritaire. Même si l'exigence de confidentialité médicale est forte, les soignants ne peuvent pas consacrer trop de temps à l'authentification, leur priorité est le patient.

Pour cette raison, certains projets hospitaliers d'authentification rencontrent peu de succès. Stations laissées en accès libre avec une carte à puce insérée en permanence, identification identique pour toute une catégorie d'utilisateurs etc.

Une solution souvent choisie : le badge sans contact avec une authentification limitée dans le temps et l'espace. Le médecin utilise un code PIN à son arrivée, puis peut accéder aux PC de son service pendant plusieurs heures en présentant simplement son badge. Cela permet d'allier sécurité et efficacité.

Contrôler l'accès aux applications

En standard, les solutions d'authentification forte ne permettent généralement pas de contrôler l'accès à des applications spécifiques, et encore moins à des ressources dans ces applications. En effet, l'éditeur d'un progiciel ne peut matériellement pas prendre en compte toutes les méthodes d'authentification possibles.

Cela est pourtant indispensable dans certains cas d'usage. Par exemple, si un médecin s'absente de son bureau avec une session ouverte, il ne faut pas qu'un tiers en profite pour émettre en son nom une prescription de médicaments. Une ré-authentification lors de la confirmation des actes est indispensable.

Une première solution : des jetons logiciels de type SAML ou Kerberos. Mais cela exige que les applications soient conçues (ou modifiées) pour les interpréter. C'est rarement le cas, et vous ne pourrez généralement pas modifier les progiciels et les applications 'historiques' de l'entreprise.

Autre solution, un outil de single sign-on (SSO) demandera une ré-authentification à chaque nouvel accès aux applications. Le SSO n'exige généralement pas de modifier vos applications – c'est donc une solution plus pratique.

Que souhaitez-vous protéger ?

La question est moins simple qu'il n'y paraît. Contrôler les accès n'est qu'un moyen pour protéger la véritable valeur de l'entreprise : informations, réputation, procédures, disponibilité opérationnelle... Ainsi, si l'on peut restreindre l'utilisation d'applications sensibles à certains PC protégés par carte à puce/badge sans contact, il sera inutile d'équiper tous les PC de l'entreprise de lecteurs de cartes/badges.

Connaître ses objectifs permet de préciser les ambitions d'un projet, qui se déclinent ensuite typiquement en fonction de cibles techniques :

1. Accès physique à des sites, des bâtiments ou des pièces,
2. Accès à distance : authentifcation sur le portail de l'entreprise,
3. Accès aux stations de travail : authentification sur un PC, un kiosque etc,
4. Accès à des applications critiques : comptabilité, trading, production...
5. Accès à des fonctions dans une application : page de signature par exemple.

Suivant les cibles, les méthodes d'authentification forte seront souvent différentes. Ainsi, rares sont les smartphones qui supportent l'insertion d'une carte à puce ! Les employés seront alors munis de plusieurs dispositifs d'authentification, ou de dispositifs multifonctions.

Authentification forte : où se trouvent les coûts cachés ?

Attention à la complexité

Les coûts de déploiement et d'usage de l'authentification forte sont généralement très supérieurs aux coûts d'achat des équipements eux-mêmes.

« 1 mécanisme, 1 utilisateur, 1 PC, 1 application ». Si votre projet consiste à équiper quelques dizaines d'employés de cartes à puce personnelles, chacune utilisée pour accéder à une application principale dans un seul PC, êtes-vous certain pour autant de ne pas rencontrer de problèmes ?

Or dans la réalité, rares sont les déploiements qui obéissent à cette règle des « 4x1 ». Et un déploiement mal préparé peut amener à des situations non prévues qui vont gêner la mise en place et augmenter les coûts d'administration.

Comment assurer une utilisation fluide et continue ?

Les concepteurs de systèmes critiques le savent : les défaillances sont inévitables ; il faut les anticiper pour qu'elles engendrent le moins de problèmes possibles. Or votre système d'information est l'un des domaines les plus critiques de votre organisation !

En ajoutant des éléments nouveaux, un déploiement d'authentification forte augmente les causes possibles de blocages d'activités cruciales – et par conséquent le nombre d'appels au help desk. Vous devez anticiper dès maintenant les problèmes les plus courants ou dommageables pour l'organisation et prévoir des réponses rapides, automatisées et peu coûteuses.

Au démarrage : utilisation des outils
Quelle que soit la simplicité apparente des outils d'authentification, vous constaterez que de nombreux utilisateurs rencontreront des difficultés. Pour anticiper cela, faites tester très tôt la solution par des utilisateurs non techniques – par exemple en implémentant un site pilote.

Ne vous cantonnez pas aux informaticiens 'aguerris', ou aux opérationnels maîtrisant l'informatique. Cela vous permettra de prévoir, si nécessaire, des séances de formation lors du déploiement.

- Les dispositifs peuvent-ils être utilisés par des employés néophytes ?
- Le fournisseur a-t-il prévu des supports pédagogiques ?

Au démarrage : procédures de sécurité
Le déploiement de l'authentification forte peut donner lieu à des failles de sécurité. En effet, vous allez attribuer des dispositifs d'authentification à des utilisateurs : il faut vous assurer que l'identité de ceux-ci soit assurée.

La meilleure façon est d'utiliser une procédure basée sur une remise en main propre, pour une bonne identification des utilisateurs.

- Comment s'assurer de l'identité de l'utilisateur auquel on remet un dispositif ?
- La vérification des droits d'accès est-elle activée dès la remise du dispositif ?

Sur la durée : perte et pannes
Les dispositifs que vous allez déployer ont un taux de panne (MTBF) connu, que pourront vous fournir les fabricants. Mais à cela, s'ajoutent les facteurs humains : dispositifs perdus ou volés, code PIN oublié, blocage automatique… ou arrêts maladie.

Les « utilisateurs influents » dont nous avons parlé en introduction sont très sensibles à ces questions. Ils veulent pouvoir continuer à travailler, même en cas de panne ou d'oubli : il faudra donc leur apporter une réponse claire et satisfaisante.

- Un employé qui a oublié sa carte peut-il recevoir un mot de passe temporaire, même si le help desk n'est pas disponible ?
- Un employé tombé malade peut-il déléguer l'accès à sa station à un collègue, sous contrôle de la politique de sécurité ?
- Peut-on gérer facilement les mises en « liste noire » de cartes ?
- Peut-on réutiliser une carte en liste noire ?

Une méthode courante est de faire l'inventaire des problèmes les plus fréquents : perte de carte à puce, panne du dispositif biométrique… mais aussi tenir compte des cas où ces problèmes surviennent alors que le help desk est indisponible.

Etude de cas
Une grande banque avait décidé de déployer une authentification biométrique par empreinte digitale auprès de ses employés. La procédure initiale exigeait que l'utilisateur enregistre trois de ses doigts – pour anticiper les cas où un des doigts ne puisse être utilisé, par exemple s'il est recouvert par un pansement.

Dans un bureau, trois utilisateurs avaient l'habitude de partager leurs PCs. Pour continuer à travailler dans ce mode peu sécurisé, ils ont simplement enregistré un doigt par personne sur chacun des PC…

Une fois le pot aux roses découvert, la procédure fut changée : désormais, l'enregistrement exige la présence d'un membre de l'équipe de déploiement.

La loi des grands nombres

Un site pilote réussi n'est jamais une garantie sans faille. Car ce qui fonctionne bien avec quelques stations et employés peut se révéler totalement inadapté pour des milliers d'utilisateurs répartis sur des dizaines de sites.

Cela s'explique par deux types de charges de gestion supplémentaires, résultant (1) de la grande quantité d'éléments à prendre en compte, et (2) de la présence de plusieurs fournisseurs avec leurs spécificités et outils d'administration souvent incompatibles.

Gérer la quantité

Introduire une grande quantité d'éléments logistiques d'authentification dans l'entreprise peut augmenter considérablement la charge de gestion. Circuits d'attribution, photographies, gestion des pertes, mots de passe temporaires en cas d'oubli, stocks de cartes, liste noire… Un système de gestion de cartes (en anglais card management system) se révèlera souvent indispensable.

Par ailleurs, un administrateur central ne peut connaître personnellement chacun des employés qu'il gère, ce qui rajoute une difficulté. Comment déterminer leurs droits d'accès individuels ? Les deux solutions classiques sont de déléguer l'administration à un niveau hiérarchique proche de l'employé, et attribuer les droits d'accès en fonction de règles métier. Souvent, ces deux pratiques coexistent : les droits d'accès déduits automatiquement sont alors confirmés par un circuit d'approbation par le manager de l'employé.

Gérer la complexité

Dans un projet, il peut être nécessaire de faire coexister de multiples fournisseurs de matériels d'authentification. Les cas d'usages peuvent exiger des matériels différents (biométrie en interne, mot de passe à usage unique en externe) qu'un seul fournisseur n'aura pas à son catalogue. De même, si des matériels existants sont déjà utilisés dans certains sites, ils pourraient être très chers de les remplacer.

Les coûts résultant de cette hétérogénéité sont souvent élevés. Ainsi, les chaînes d'approvisionnement des équipements sont dupliquées, ainsi que les interfaces d'administration utilisées au quotidien. Enfin, changer de fournisseur devient extrêmement coûteux, ce qui nuit aux négociations.

L'objectif est de rechercher des solutions permettant de rendre le système le plus ouvert possible envers les technologies utilisées. Ainsi, certains logiciels de gestion d'authentification présents sur les PC peuvent accueillir des équipements de plusieurs fournisseurs, et apportent des fonctions supplémentaires telles que l'obtention de mots de passe temporaires par questions/réponses, sans appeler le help desk. De même, des outils tierce-partie de gestion de cartes peuvent accueillir des cartes de nombreux fournisseurs.

Etude de cas

Un équipementier automobile voulait permettre à plus de 20 000 employés d'utiliser la même carte personnelle pour entrer dans ses sites, payer à la cantine et accéder à leur PCs. L'intérêt était clair : si les employés ont besoin d'avoir leur carte toujours avec eux, ils ne peuvent la laisser en permanence branchée à leur PC.

Dans la phase de préparation, l'entreprise a réalisé que la plupart de ses sites étaient équipés de systèmes de contrôle d'accès physique. L'entreprise a rapidement réalisé qu'il n'y avait aucune homogénéité dans ces équipements :
comment dans ce cas déployer une solution internationalement ?

La solution a été de faire appel à un intégrateur spécialisé, qui a adapté au cas par cas les badges des employés pour faire coexister leur composant « sans contact » avec une puce d'authentification standardisée. Le projet a également intégré un composant de gestion des badges.

Les cas particuliers d'utilisation

Dans les déploiements d'authentification forte, la découverte de cas d'usage particulier non couverts par la solution peut mener à son rejet par des utilisateurs. Ce risque est d'autant plus grand que les utilisateurs qui ont des contraintes spécifiques sont souvent particulièrement influents. Vous trouverez ci-dessous plusieurs de ces situations, avec les points à exiger de vos solutions d'authentification.

Un utilisateur – utilisant plusieurs PC successifs

Les tâches quotidiennes de certains employés peuvent les amener à se déplacer dans un site : médecins en hôpital, gestion de production dans un site industriel, vendeurs en magasin etc. Dans ce cas, des PC en « kiosque » sont souvent disponibles – l'employé doit pouvoir s'authentifier et retrouver rapidement sa session de travail, quel que soit le point d'accès sur le site.

- Après une authentification, l'employé retrouve-t-il son environnement de travail en quelques secondes, sans attendre un redémarrage de session ?
- Peut-on interdire l'usage des PC en kiosque à certaines catégories d'employés, et sur certaines zones du site ?
- La solution fonctionne-t-elle avec des badges sans contact, ou des cartes à puce professionnelles ou gouvernementales ?

Un utilisateur – accédant depuis plusieurs zones

Un utilisateur peut vouloir accéder à ses ressources lors de ses déplacements sur plusieurs sites de l'entreprise. Les employés accèdent de plus en plus aux applications professionnelles avec leur smartphone ou leur PC personnel. Il faut pouvoir contrôler ces accès sans pour autant empêcher ces utilisateurs de travailler.

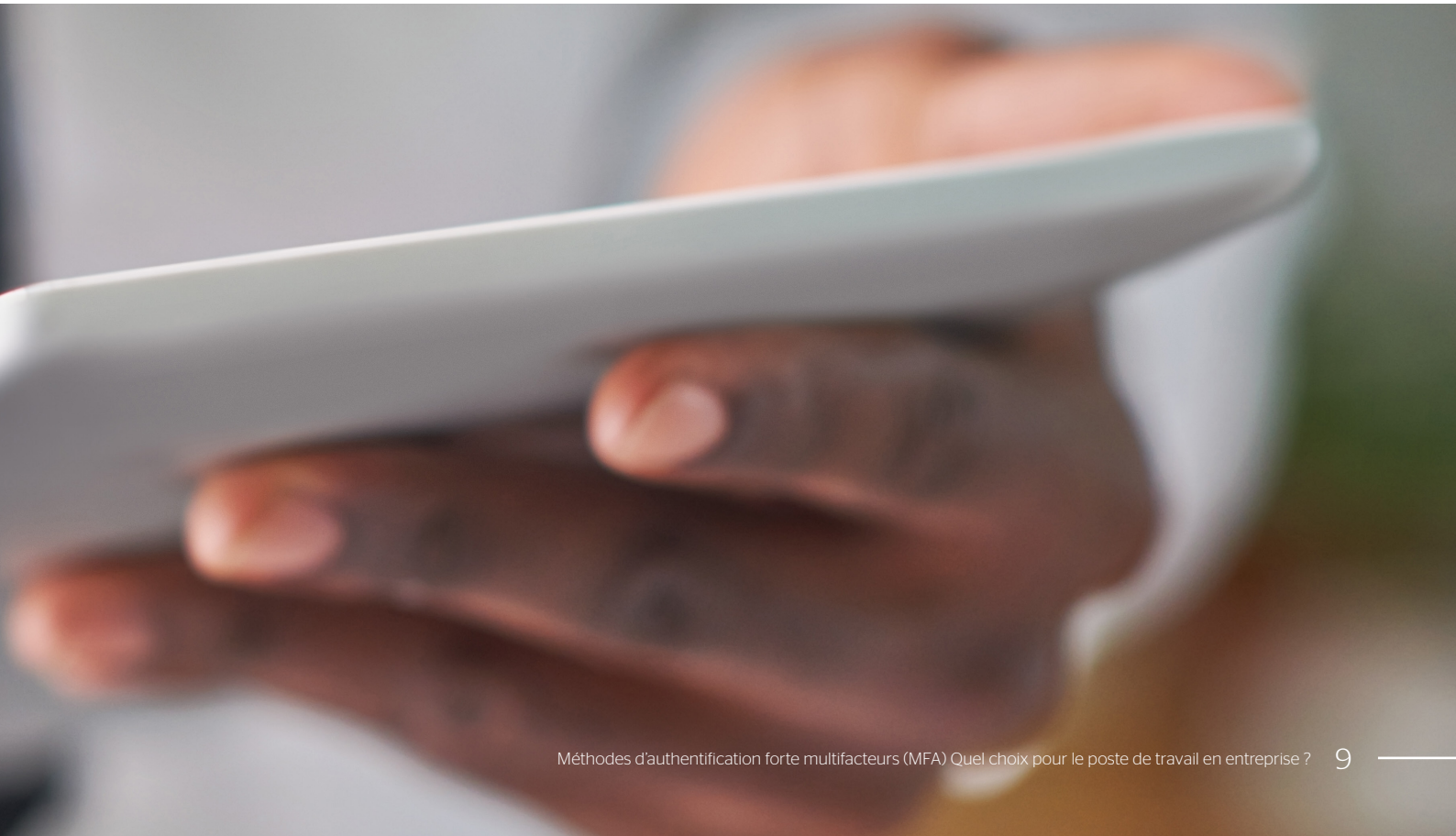
- Peut-on donner des droits d'accès à un utilisateur sur plusieurs sites géographiques de l'entreprise ?Les PC de sites distants sont-ils configurés pour accueillir la solution d'authentification ?
- L'utilisateur peut-il s'authentifier sur un PC portable déconnecté ?
- Comment s'authentifie un utilisateur s'il veut accéder aux ressources sur son smartphone ?

Un utilisateur – utilisant plusieurs PC à la fois

Certains de vos employés ont besoin de plusieurs PCs et écrans pour travailler. Ingénieurs de développement logiciel, traders en salles de marchés, surveillance d'exploitation industrielle… Il est peu réaliste de leur demander de se connecter (et se déconnecter) successivement sur tous leurs postes.

- Une seule authentification permet-elle de débloquer (puis de verrouiller) tous les postes de l'utilisateur ?
- Comment l'utilisateur peut-il déléguer l'accès à un collègue ou un assistant à sa « grappe » de stations de travail ?
- Peut-on garder certains écrans en mode 'surveillance' (affichage actif sans clavier ni souris) pendant l'absence de l'utilisateur ?

Nous l'avons vu, il est important que les cas les plus critiques soient couverts. Une solution fréquemment utilisée est de décrire des scénarios d'utilisation dans les phases initiales du projet. Recueillez les avis des parties prenantes et faites-leur valider ces scénarios. Vous disposerez ainsi d'une adhésion par les utilisateurs et de fiches de test pour les pilotes et la phase de choix du fournisseur.



Etude de cas
Une banque internationale souhaitait s'assurer, pour chaque opération effectuée en salle de marchés, de l'identité du trader responsable. L'objectif était d'éviter que l'auteur d'une opération puisse nier l'avoir effectuée.

Le problème : en salle de marchés, l'accessibilité des stations est extrêmement importante. Il n'est pas question de rater une opportunité parce que l'on a passé plusieurs secondes à renseigner un mot de passe. Comment dans ce cas faire accepter un système de contrôle d'accès par les traders ?

La banque a donc travaillé avec Evidian pour passer en revue toutes les procédures de salle de marchés, en s'assurant pour chacune que la solution d'authentification ne gênerait pas les opérations. Cela a permis de déployer la solution de contrôle d'accès dans tous les pays.

Les restrictions techniques

Certaines solutions d'authentification ont des limites en termes d'utilisation. Une limitation technique peut être intrinsèque : ainsi, certaines solutions de virtualisation de stations ne gèrent pas nativement les cartes à puce ou la biométrie. Il faut alors prévoir une solution séparée de gestion des authentifications.

Les limitations sont parfois moins évidentes : ainsi, une grande entreprise pétrolière a dû choisir des cartes à puce résistantes aux hautes températures pour équiper ses employés travaillant dans les pays du Golfe. Autre exemple, des contraintes légales empêchent l'usage de certaines solutions, comme les règlements sur l'export d'algorithmes de chiffrement.

On le voit, certaines limitations techniques risquent de ne pas être révélées par un site pilote. Si elles sont découvertes en cours de déploiement, il pourra être nécessaire de prévoir des solutions alternatives pour certains pays, départements ou catégories d'utilisateurs.

Il est donc particulièrement utile de détailler des cas d'usage avant le choix des solutions.

Si l'architecture de la solution globale ne dépend pas du fournisseur d'authentification forte, ce sera donc là aussi un atout. Il sera plus facile de trouver des solutions palliatives chez un autre fournisseur en cas de problème.

Etude de cas
Une grande institution financière souhaitait protéger les PC de tous ses chargés de clientèle par une vérification d'empreinte digitale. Mais cette solution se heurte à des limites légales. En France, la loi interdit en effet de centraliser le stockage de la plupart des signatures.

La solution : équiper les employés de cartes à puce contenant les signatures biométriques. Une procédure simple permet à l'employé d'enregistrer ses empreintes digitales pour les lier à son compte Windows. Suite à cela, la carte (et le doigt de l'employé) sont nécessaires pour se connecter.

Récapitulatif

Un déploiement de contrôle d'accès sera réussi et peu coûteux dans la durée, s'il est soigneusement préparé en anticipant tous vos cas majeurs d'utilisation – qu'ils soient habituels ou occasionnels. Cela permettra d'éviter les obstacles au déploiement, qu'ils soient de nature technique, organisationnelle ou humaine.

En envisageant la gestion quotidienne dès le démarrage du projet, vous vous assurerez que l'authentification forte sera acceptée par les utilisateurs et n'occasionnera pas de surcoûts imprévus d'exploitation.

Pour plus d'informations, visitez notre wite web : www.evidian.com

Découvrez notre solution Evidian Authentification Manager pour l'authentification forte et l'authentification multifacteurs -MFA :
https://www.evidian.com/products/authentication-manager/

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 logiciels 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'Evidian.

© 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_180703_EM_WP-MÉTHODES-AUTHENTIFICATION-(MFA)-FR