LIVRE BLANC

Authentification forte

Comment obtenir le niveau de protection des identités dont vous avez besoin, de façon à la fois pratique et abordable

Résumé opérationnel

Accommoder tous les différents besoins en matière d'accès logique de tous les utilisateurs, tout en verrouillant simultanément vos ressources pour les protéger contre les menaces, est un défi constant.

Pour être sûr que vos utilisateurs sont bien ceux qu'ils prétendent et qu'ils gèrent efficacement leur accès à vos ressources, vous avez besoin d'une solution de protection des identités complète, sur laquelle repose l´authentification forte.

Toutefois, l'émission et la gestion continue des moyens d'identification des utilisateurs, sur tous les divers appareils, des cartes à puce aux téléphones mobiles que vous devez prendre en charge, pour toutes les applications et ressources auxquelles vos utilisateurs peuvent vouloir accéder, peuvent poser leurs propres problèmes. De ce fait, il vous faut une solution d'authentification forte qui facilite l'émission et la gestion des moyens d'identification en vue de fournir différents niveaux d'accès d'une façon commode pour l'utilisateur. Toute procédure qui ne respecterait pas ce minimum aurait un impact négatif sur l'efficacité de la solution complète.

Sommaire

Le besoin d'une authentification forte dans l'entreprise d'aujourd'hui

Les utilisateurs sont de plus en plus dispersés géographiquement, mobiles et variés, ce qui oblige de nombreuses entreprises à s'intéresser aux moyens d'établir la confiance dans l'identité des utilisateurs et de contrôler leur accès en conséquence. Par le passé, la plupart d'entre elles se concentraient sur les défenses périphériques, mettant en place des contrôles pour déterminer qui pouvait entrer dans le bâtiment, avec des systèmes d'accès physique, et qui pouvait entrer sur le réseau grâce à des pare-feux et des VPN. Une fois à l'intérieur, les utilisateurs avaient un accès quasiment illimité à toutes les applications et ressources disponibles dans ces sites et ces réseaux.

À présent, reconnaissant les menaces que les utilisateurs représentent « à l'intérieur des murs » (81 % des entreprises ont en effet subi une violation des données du fait de salariés ou autres personnes se trouvant sur place, aussi bien par négligence que par malveillance) et observant que les murs, eux-mêmes, tombent du fait de la nature mondiale et dynamique des entreprises actuelles, de nombreuses entreprises revoient leur approche en matière d'accès logique.

Si vous êtes comme la plupart des entreprises, vous luttez pour accommoder simultanément les différents besoins de tous vos différents utilisateurs et vous cherchez à minimiser les risques que pose leur accès à votre organisation, ce qui est rendu compliqué par l'évolution permanente du panorama des menaces et le nombre d'utilisateurs. Les attaques continuent d'évoluer et deviennent de plus en plus complexes, comme le montre la montée des menaces avancées et persistantes qui utilisent des logiciels malveillants personnalisés pour mener des attaques ciblées à long terme contre votre organisation. Parallèlement, les utilisateurs qui ont besoin d'accéder aux informations et aux ressources, ne se limitent pas aux salariés et incluent un large éventail de consultants, contractants, fournisseurs, partenaires, fournisseurs et clients.

Tous ces utilisateurs veulent pouvoir accéder à ce dont ils ont besoin, peu importe d'où ils viennent, en utilisant l'appareil de leur choix, y compris leurs téléphones personnels, ordinateurs portables et tablettes (BYOD). Ces variables peuvent accroître les risques pour votre environnement si vous ne faites pas attention. Ce qu'il vous faut, c'est une méthode permettant de s'assurer de l'identité de tous ces utilisateurs différents, puis de contrôler de façon adéquate leur accès tout au long de leurs déplacements dans l'organisation.

Appliquer une authentification forte à chaque application est l'un des moyens les plus efficaces pour obtenir la productivité dont votre activité à besoin, tout en réduisant les risques pour votre entreprise. En assurant les applications et les ressources de données de l'entreprise et basées sur le cloud, qu'elles soient sur un ordinateur portable ou un téléphone mobile, vous pouvez gérer efficacement l'accès et sécuriser vos systèmes d'informations.

Définir l'authentification forte pour traiter les défis posés par les solutions traditionnelles

Une authentification forte, parfois appelée authentification avancée ou authentification double facteur, va bien au-delà d'un simple mot de passe d'authentification. Elle requiert des facteurs supplémentaires pour établir que l'utilisateur est qui il est. Il peut s'agir de quelque chose que l'utilisateur sait, comme un mot de passe unique ou un numéro d'identification personnel (PIN) ; quelque chose que l'utilisateur a, comme une carte à puce, un token ou un téléphone portable ; ou même quelque chose que le système d'authentification collecte, comme une connaissance des fraudes et des comportements, qui sert à augmenter le niveau de sécurité de l'authentification.

Pourquoi est-ce important ? Les hackers continuent de cibler les moyens d'identification des personnes qui se trouvent à l'intérieur des bâtiments parce qu'ils donnent à l'attaquant un accès aux sites et au réseau, leur permettant de se « fondre dans la masse », de sorte qu'ils peuvent aller et venir dans l'entreprise sans se faire détecter. De récentes études indiquent que près de 50 % des violations de données exploitent les systèmes d'identification volés ou faibles. Cela dit, il est facile de voir à quel point la solidité croissante des authentifications de vos utilisateurs peuvent vous aider à renforcer la sécurité générale de l'entreprise.

La réalité repose sur l'utilisation de mots de passe statiques traditionnels qui, bien que pratiques, ne sont pas suffisants pour protéger contre les menaces dynamiques actuelles ; les outils de capture de frappe, les attaques d'hameçonnage, les écoutes et même le fait de deviner peut facilement servir à les briser. Les mots de passe à usage unique (OTP) et tokens offrent une sécurité supérieure, car le mot de passe qu'ils génèrent n'est valide que pour une seule session ou transaction, mais s'ils sont implémentés de façon incorrecte, ils peuvent créer d'autres problèmes. De nombreuses solutions héritées ne vous donnent pas de contrôle sur la clé du token ; au lieu de cela, les clés sont hébergées dans les bases de données du fournisseur, ce qui signifie qu'une violation chez celui-ci peut endommager la sécurité de votre entreprise.

De plus, les solutions héritées qui partent du principe qu'une fois que vous êtes entré, il n'y a aucun problème, ne sont pas suffisamment complètes ou polyvalentes pour prendre en considération le rôle de l'utilisateur, le lieu et le type d'accès en vue d'établir la confiance et de garantir l'accès à un vaste éventail d'applications dans l'entreprise et dans le cloud. Il ne suffit plus d'utiliser une authentification forte quand vous entrez dans le bâtiment ou le réseau pour la première fois. Comme indiqué, il n'y a plus de périmètre défendable. Une authentification forte doit être étendue dans toute l'organisation pour inclure l'accès aux bureaux, serveurs, téléphones portables, données, ainsi qu'aux applications d'entreprise et dans le cloud, d'une façon qui vous permette de renforcer la sécurité générale et la responsabilité de votre environnement.

Toutefois, l'émission et la gestion continue des moyens d'identification des utilisateurs, sur tous les divers appareils, des cartes à puce aux téléphones mobiles, pour toutes les applications et ressources auxquelles ils peuvent vouloir accéder, peuvent représenter un processus manuel chronophage. Cela se complique encore plus lorsqu'il y a plusieurs types de moyens d'identification, pour l'accès physique et logique, et différents systèmes d'identification et d'authentification. Il faut un processus unique, reposant sur un système de gestion des utilisateurs et des moyens d'identification consolidés, capable d'émettre et de gérer les systèmes d'identification de tous vos utilisateurs pour leur accorder un accès adéquat à tout, des bâtiments aux applications dans le cloud, via différents facteurs de forme, depuis des cartes à puce jusqu'à des téléphones portables.

Polyvalence du dispositif ActivID en un clin d'œil

- **Prise en charge des périphériques :** smart phones, tablettes, ordinateurs portables, etc.
- **Méthodes d'identification :** hard tokens (jetons matériels) et soft tokens (jetons logiciels) de mot de passe à usage unique, cartes à puce, périphériques d'identification, authentification adaptative, mécanismes de détection des fraudes, et mécanismes hors-bande (SMS ou e-mail) pour une authentification au niveau des transactions
- **Applications :** Entreprises, Cloud, etc., comme Windows, Salesforce.com, SAP, Oracle, Google Apps, etc.

Critères pour une authentification forte efficace - sans compromis

Une solution d'authentification forte efficace doit pouvoir ajouter de la sécurité sans accroître les coûts ou la complexité. Pour les environnements professionnels actuels, seule une solution d'authentification forte, facile à utiliser et simple à gérer a une chance de fonctionner avec l'ensemble des utilisateurs que votre organisation doit prendre en compte pour vous protéger contre les nombreuses attaques connues et à venir. Vous avez besoin d'une solution qui vous fournit :

Authentification forte :

- **Double facteur ou plus :** augmente le niveau de confiance que vous avez dans les identités de vos utilisateurs, de sorte que vous puissiez leur octroyer un accès adéquat.
- **Différents niveaux d'accès :** basés sur les risques associés aux différents types d'utilisateurs et de transactions. Vous devriez pouvoir être en mesure de fournir des capacités de sécurité à couches multiples et transparentes pour accroître considérablement votre sécurité, sans que cela n'ait d'incidence sur l'expérience des utilisateurs (au moins pas ceux qui se connectent à partir de leurs périphériques et lieux de confiance). Cela peut être obtenu grâce à des solutions capables de :
- **Détection avancée des fraudes :** tenez compte de facteurs tels que la situation géographique et les informations relatives aux périphériques quand vous authentifiez des utilisateurs, afin de pouvoir limiter l'accès à des périphériques de confiance, dans des pays de confiance.

Sinon, les utilisateurs peuvent être conviés à utiliser une méthode d'authentification supplémentaire plus sûre, comme un mot de passe unique envoyé par SMS, en cas de connexion à partir de périphériques ou de sites qui ne figurent pas sur la liste de confiance.

- **Analyse continue des comportements :** pour une authentification continue et une amélioration des capacités de recherche de preuves, à l'aide de l'analyse comportementale des interactions d'un utilisateur avec les applications. L'activité de l'utilisateur est constamment surveillée et analysée, pour savoir comment un utilisateur particulier se comporte, de sorte que les conclusions tirées de ce comportement puissent être détectées et signalées, sans avoir d'incidence sur l'expérience de l'utilisateur ou mettre en danger la confidentialité.

Si une déviation se produit (par exemple, si quelqu'un a pris la main sur l'ordinateur), l'application peut choisir de redemander à l'utilisateur de s'authentifier et/ou ajouter un événement à une base de données d'audit pour étude ultérieure. Cette méthode peut en fait servir à réduire le nombre de tentatives nécessaires pour qu'un utilisateur s'authentifie auprès d'un système afin d'améliorer son confort.

Gestion simplifiée :

- **Rapide à déployer et à administrer :** il devrait être facile d'obtenir que la solution soit en place et fonctionne, sans ajouter de complexité ou de coûts inutiles. Dans l'idéal, elle devrait vous permettre d'avoir une vue groupée pour simplifier l'émission des moyens d'identification et la gestion continue de vos solutions de protection des identités afin de garantir qu'elles prennent en charge votre position en matière de sécurité (par exemple, il devrait être facile d'identifier et de révoquer des moyens d'identification, de façon à ce que vous n'ayez pas de moyen d'identification actif pour un salarié qui a quitté votre entreprise).
- **Complet :** système de gestion des identifications simple, capable de gérer vos moyens d'identification des utilisateurs sur plusieurs dispositifs, comme des cartes à puce et téléphones portables, et le cycle de vie continu de ces moyens d'identification et dispositifs. Dans l'idéal, il devrait vous permettre d'accéder aussi bien à vos actifs physiques (bâtiments) que logiques (applications et ressources d'entreprise et dans le cloud) et fournir une vue groupée unique de tous vos systèmes de protection des identités.
- **Intégration facile :** la solution doit être en mesure de s'intégrer aux outils de gestion continue que vous utilisez normalement pour créer une interface utilisateur consolidée et stable afin d'administrer l'authentification et les systèmes d'identification de sécurité des utilisateurs.

Confort de l'utilisateur :

- **Facile à utiliser :** ne devrait pas gêner les flux de travail. Dans l'idéal, la solution devrait utiliser les badges d'identification existants, cartes à puce ou téléphones portables des utilisateurs pour étendre l'accès sécurisé aux ressources physique et logique dont l'utilisateur a besoin.
- **Continuité :** ne devrait pas provoquer de retard indu pour les applications d'entreprise et basées sur le cloud dont les utilisateurs ont besoin pour mener leurs activités.

L'approche pour une solution d'authentification forte capable de fournir aux utilisateurs l'accès sécurisé dont ils ont besoin

Le portefeuille de produits ActivID™ peut être utilisé pour émettre et administrer des systèmes d'identification servant à l'ensemble des utilisateurs qui ont besoin d'accéder à votre réseau, et leur permettre d'utiliser tout dispositif en vue de s'authentifier pour utiliser les ressources dont ils ont besoin d'une façon à la fois pratique et sûre. La solution puissante repose sur le système d'identification convergé ActivID, le serveur d'authentification de l'appliance ActivID et le système d'administration des moyens d'identification (credential management system, ou CMS) d'ActivID :

Support d'identification convergé :

Le portefeuille ActivID fournit le seul moyen d'identification convergé de l'industrie pouvant être intégré dans une carte à puce, un badge d'identification ou même un téléphone portable et pouvoir servir aussi bien à des systèmes physiques que logiques pour permettre aux utilisateurs de s'authentifier afin d'entrer dans un bâtiment, d'ouvrir une session sur le réseau, et d'avoir un accès sécurisé aux applications et autres systèmes dont ils ont besoin. Ils peuvent également utiliser le moyen d'identification convergé pour accéder à des réseaux sécurisés, remplaçant ainsi le besoin d'un token ou porte-clé de mot de passe à usage unique.

Un moyen d'identification convergé est plus pratique pour les utilisateurs car il élimine le besoin de transporter plusieurs dispositifs ou d'émettre à nouveau des mots de passe à usage unique. Il fournit également une sécurité considérablement renforcée, en activant une authentification forte dans l'ensemble de l'infrastructure informatique sur les systèmes-clés, les ressources de l'entreprise et les applications basées sur le cloud, plutôt que de se concentrer uniquement sur la périphérie.

Dispositif ActivID CMS en un coup-d'œil :

Vous pouvez gérer vos :

- **Dispositifs d'authentification** : depuis les cartes à puce jusqu'aux tokens USB en passant par les téléphones portables
- **Données** : mots de passe statiques, solutions biométriques et données démographiques
- **Applets** : applications à mot de passe à usage unique et applets de vérification de l'identité personnelle
- **Identifiants numériques** : y compris des certificats d'infrastructure de clé publique [PKI] tout au long de leur cycle de vie

Serveur d'authentification du dispositif d'ActivID :

Le serveur d'authentification de l'appliance ActivID vous procure la polyvalence dont vous avez besoin pour procéder à l'authentification de façon pratique et économique, et protéger l'accès à vos utilisateurs vers les applications dont ils ont besoin pour leur travail. En prenant en charge divers dispositifs et plus de quinze méthodes d'authentification, il vous procure ce qu'il vous faut pour avoir confiance dans l'identité de vos utilisateurs afin de leur accorder un accès sécurisé à toutes les applications de votre entreprise et basées sur le cloud.

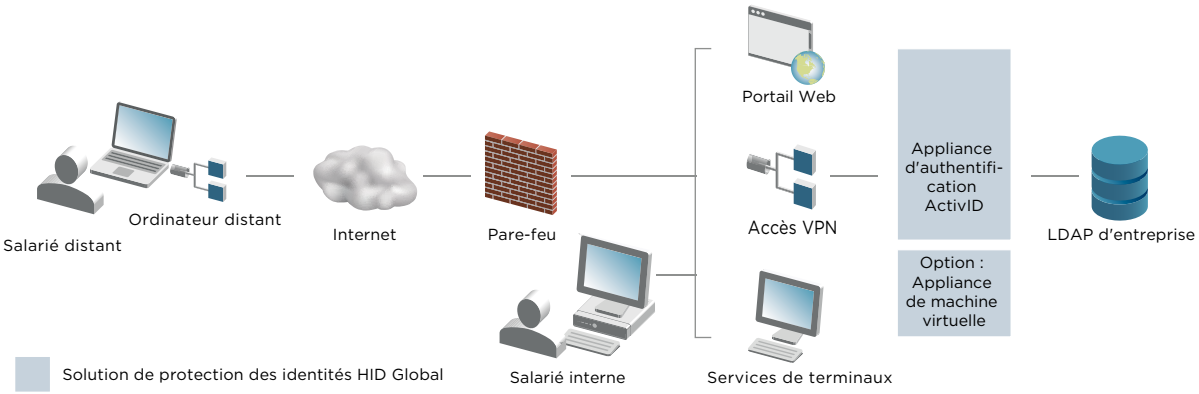
L'appliance ActivID vous fournit la sécurité dont vous avez besoin, en vous épargnant la complexité. Les modèles et stratégies faciles à définir vous permettent de déployer facilement une solution d'authentification qui répond à vos besoins. Le service unique de détection des fraudes de l'appliance ActivID vous permet de personnaliser la solution en fonction des critères spécifiques de votre environnement. Il peut servir à identifier les détails des accès, comme l'ordinateur à partir duquel les utilisateurs se connectent, le navigateur qu'ils utilisent, et s'ils l'ont déjà utilisé par le passé, pour que vous soyez en mesure de déterminer si une authentification simple est garantie ou s'il convient d'utiliser une authentification double facteur à ce moment-là, en vous appuyant sur votre ensemble de règles prédéfinies. Cela vous permet de renforcer la sécurité de façon simple pour vous et invisible pour l'utilisateur.

Vous pouvez vous montrer aussi spécifique que vous le voulez, limiter l'accès à des dispositifs particulier dans une zone particulière, ou voir la fonction occupée par l'utilisateur (n´importe qu´il soit le PDG ou un responsable marketing) et déterminer le moyen d'identification à utiliser et la manière de traiter l'accès. Vous pouvez également bénéficier des informations collectées par des milliers d'autres clients pour savoir si l'évolution du paysage (par exemple, si le comportement des ordinateurs d'un secteur particulier est signalé) doit modifier vos critères d'authentification (limiter l'accès ou imposer une authentification supplémentaire).

De ce fait, ActivID vous aide à devancer vos critères en constante évolution, protégeant la sécurité d'une façon qui se fond avec les flux de travail de vos utilisateurs pour garantir que vous pouvez renforcer la protection autour de vos actifs critiques. ActivID peut vous aider à être conforme aux normes FFIEC actualisées, PCI DSS et autres législations, stratégies et directives relatives au commerce/opérations bancaires en ligne dans le monde. Notez que les tokens ActivID durent jusqu'à huit ans et que vous pouvez administrer vos propres ensembles de clés pour conserver un contrôle complet sur la protection et les clés de chiffrement pour plus de tranquillité.

Les services professionnels de HID Global sont également disponibles pour vous aider à affiner l'implémentation et la configuration du service de détection des fraudes de l'appliance ActivID si besoin. Ils peuvent vous aider à développer les meilleures stratégies pour votre environnement en prenant en compte n'importe lequel de la vingtaine de paramètres à votre disposition, depuis le rôle et l'heure à laquelle les gens se connectent, jusqu'au lieu et au type d'appareil, etc., pour faciliter l'installation et accélérer l'exécution.

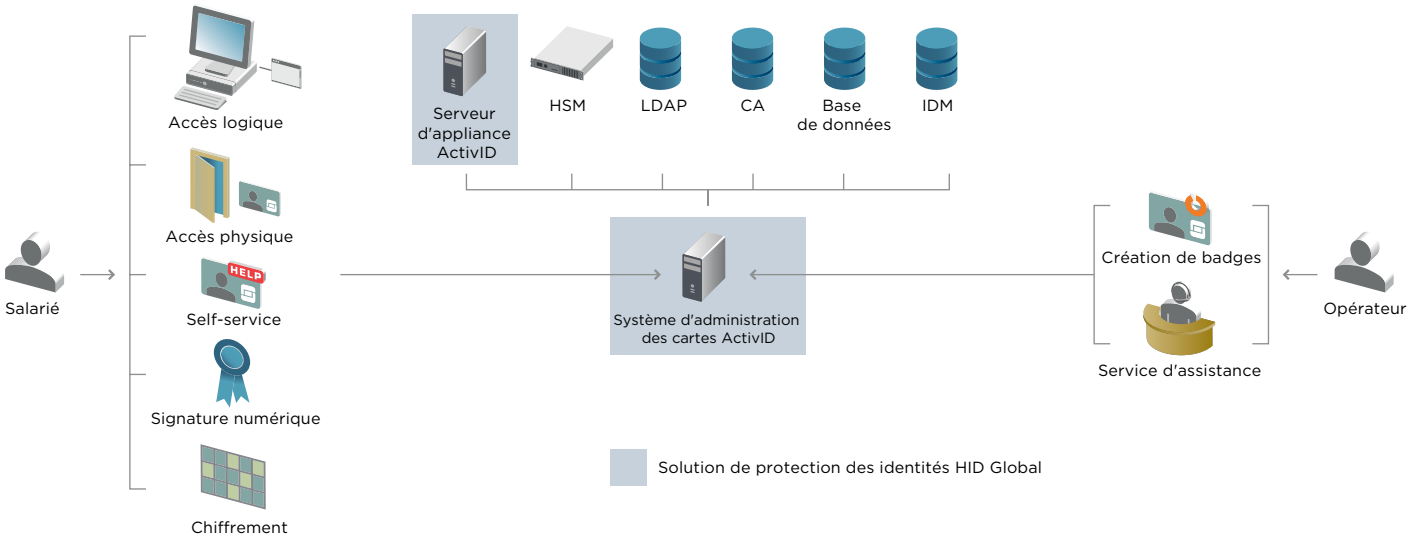
Authentification de dispositifs d'ActivID : mode de fonctionnement



Système de gestion des cartes ActivID

Le CMS d'ActivID fournit une solution complète et flexible pour vous permettre d'administrer facilement les critères d'émission et d'administration des déploiements d'authentification réussis. Vous pouvez émettre et administrer des cartes à puce, des tokens USB à puce et des tokens sur téléphones portables pouvant servir à un large éventail d'applications de bureau, de sécurité réseau et de productivité. Cela vous permet de configurer des flux de travail et stratégies personnalisables capables de s'adapter à tous vos environnements et scénarios de déploiement. Il fournit des fonctions d'audit complètes et inviolables qui enregistrent toutes les activités des événements pour la création de rapports, avec des capacités de mise à jour après émission uniques et brevetées pour vous aider à maintenir votre solution d'authentification en vigueur. Le self-service basé sur le Web et l'administration du service d'assistance réduisent les coûts d'exploitation associés à la gestion continue et à la maintenance de la solution.

Système de gestion des cartes ActivID : mode de fonctionnement



Récolter les avantages d'une solution d'authentification forte efficace

La solution complète d'authentification forte AcvitvID vous aide à accroître votre sécurité, tout en répondant aux besoins de vos utilisateurs divers, mobiles et géographiquement dispersés. La flexibilité de la solution vous permet d'équilibrer vos critères de coûts et de sécurité, de sorte que vous puissiez délivrer le confort que vos utilisateurs recherchent et limiter les risques posés par les menaces en constante évolution. La solution ActivID fournit :

Authentification forte :

- **Diminution des risques :** connectez en toute sécurité les utilisateurs à des applications via une authentification à deux facteurs ou plus, pour éviter les violations
- **Détection des fraudes et analyse des comportements :** fournissez des facteurs supplémentaires à prendre en considération dans le processus d'authentification pour élever votre niveau de confiance dans l'identité et l'accès de vos utilisateurs et améliorez l'expérience d'ensemble de vos utilisateurs
- Stratégie d'authentification adaptative : peut déterminer différents niveaux d'accès, en définissant les moyens d'authentification (dispositif) dont quelqu'un a besoin et le type d'accès requis

Gestion simplifiée :

- **Rapide à déployer et à administrer :** les utilisateurs ne perdent pas de temps grâce à l'authentification par token qui permet de sécuriser leurs applications dans l'ensemble de l'organisation.
  - Au fur et à mesure que les besoins de l'organisation évoluent, une mise à niveau de licence simple fournit aux organisations un accès au choix de méthodes d'authentification le plus vaste du secteur, avec notamment des solutions basées sur des certificats, des connaissances et des risques.
  - Inclut des stratégies de sécurité et processus d'entreprise faciles à définir pour émettre et administrer des moyens d'identification numériques et des dispositifs au sein de groupes d'utilisateurs illimités dans des lieux géographiquement dispersés.
- **Coûts réduits :** un moyen d'identification convergé et unique élimine le besoin d'investir dans des infrastructures d'authentification physiques et logiques distinctes ; simplifie les processus, réduit la paperasse et facilite l'administration générale de votre solution de protection des identités.
  - Étend les capacités sur le badge ou le téléphone portable d'un utilisateur, élimine le besoin de mots de passe et tous les processus liés à leur réinitialisation, etc.
  - Une plate-forme d'authentification versatile, muti-couches, vous permet de minimiser le temps et les coûts liés au déploiement et au maintien des identités numériques sous la forme de cartes à puce, tokens USB et téléphones portables.
  - Vous pouvez réserver vos dépenses de sécurité aux utilisateurs et applications qui en ont le plus besoin.
- **Valeur étendue :** une plate-forme d'administration complète, hautement modulable et configurable pour les badges multifonctions des salariés, supports d'identification basés sur une carte à puce et tokens sur des téléphones portables.
  - Sécurisez l'accès via smartphones, iPad, ordinateur portable et PC aux VPN, portails Web et applications dans le cloud
  - S'intègre facilement à un large éventail de systèmes d'exploitation, répertoires, systèmes d'administration et de provisioning front-end ou back-end, autorités de certificats, et systèmes de contrôle d'accès physique
  - Emploie une authentification basée sur les normes OATH entièrement interopérable, étendant ainsi le choix des périphériques d'authentification

Confort de l'utilisateur :

- **Utilisation facile :** un simple badge d'identité ou même le téléphone portable de l'utilisateur peut servir aussi bien pour l'accès physique que logique. Avec rien d'autre à transporter ou à mémoriser, l'intégration avec les flux de travail actuels est facile.

Accroît la productivité :

- Des mesures de sécurité invisibles, comme la détection des fraudes et l'analyse des comportements, rendent la solution transparente pour l'utilisateur et peuvent réduire le nombre de fois où l'utilisateur doit s'authentifier.
- Les stratégies peuvent élever les mesures de sécurité d'après le niveau de risque et d'exposition pour l'entreprise. Cela garantit une diminution des étapes supplémentaires et que celles-ci ne sont requises que lorsqu'elles sont garanties (étant donné un certain nombre de facteurs, comme le lieu, le type de dispositif, la fonction occupée, l'heure, les modifications de comportement, etc.).

La différence ActivID : tranquillité d'esprit pour les utilisateurs et les organisations

Pour les environnements dynamiques actuels, seule une solution d'authentification forte, facile à utiliser et simple à administrer peut répondre aux critères à la fois des utilisateurs et de votre organisation. La solution ActivID vous apporte la flexibilité nécessaire pour prendre en charge et sécuriser le nombre important d'utilisateurs au sein de votre entreprise, et les divers appareils qu'ils utilisent pour accéder aux nombreuses ressources et applications. Elle est utilisée par un grand nombre des organisations les plus sensibles à la sécurité, depuis le Ministère de la défense américain jusqu'aux institutions financières et de santé. Offrant les seules solutions d'accès véritablement convergées sur le marché, HID Global vous fournit la solution Identity Assurance la plus complète, qui va du badge d'accès pour lecteur de porte à l'appliance et au logiciel d'authentification. Grâce à son déploiement, vous pouvez élever le niveau de confiance que vous avez dans l'identité de vos utilisateurs et protéger efficacement votre organisation contre les risques actuels et à venir. De ce fait, vous pouvez connecter en toute sécurité des utilisateurs à partir de n'importe quel endroit, via divers dispositifs et méthodes d'authentification pour les aider à obtenir ce dont ils ont besoin de façon commode, quand ils en ont besoin pour faire avancer votre activité en toute confiance.

À propos de HID Global

HID Global est une source fiable de produits, services, solutions et savoir-faire innovants liés à la création, l'utilisation et la gestion d'identifications sécurisées pour des millions de clients dans le monde. L'entreprise dessert notamment, les marchés suivants : le contrôle d'accès physique et logique avec authentification forte et gestion des informations d'identification, l'impression et la personnalisation de cartes, la gestion des visiteurs, les systèmes sécurisés de production de cartes d'identité professionnelles des administrations publiques ou de cartes nationales d'identité, les technologies RFID utilisées pour l'identification des animaux et les applications industrielles et logistiques. Les principales marques sont ActivId®, EasyLobby®, FARGO® et HID®. Avec son siège social établi à Irvine, en Californie, HID Global compte plus de 2 000 salariés dans le monde et possède des filiales dans plus de 100 pays. HID Global® est une marque du groupe ASSA ABLOY. Pour de plus amples informations, veuillez consulter le site **www.hidglobal.fr.**