WHITE PAPER

Sécuriser l'accès des appareils mobiles personnels à l'informatique de l'entreprise et aux éléments dans le cloud grâce à une authentification forte

Une authentification forte est la base pour sécuriser l'accès mobile

Résumé analytique

La consumérisation de l'informatique oblige les entreprises à revoir la manière dont elles établissent la confiance dans les identités des utilisateurs et accordent un accès à leurs ressources et aux applications dans le cloud, car un nombre croissant d'utilisateurs apportent leur propre appareil au travail et demandent un support de la part de leurs services informatiques. Lorsqu'elles veulent protéger l'accès à partir de ces appareils mobiles, dont un grand nombre ne leur appartient pas ou échappent à leur gestion, les entreprises doivent réussir à équilibrer les coûts, la praticité et la sécurité. Avec HID Global, les organisations avoir confiance dans les identités de leurs utilisateurs lorsqu'ils accèdent à des ressources à partir de leurs appareils mobiles, puis gérer cet accès en vue de protéger l'entreprise et les applications dans le cloud. HID Global fournit depuis longtemps des solutions de confirmation d'identité complètes et innovantes pour garantir aux organisations qu'elles respectent bien leurs exigences en matière de sécurité et de coûts, tout en répondant également aux attentes de leurs utilisateurs.

Un monde mobile - par les nombres :

- Une étude réalisée par Accenture a conclut que 83 % des entreprises estiment que la mobilité va avoir un impact important sur leur activité.
- Gartner prédit qu'un milliard de smartphones seront livrés en 2013.
- Apple a vendu 67 millions d'iPads en moins de deux ans. Il a fallu 24 ans à Apple pour vendre le nombre équivalent d'ordinateurs Macintosh.
- D'ici 2016, l'échange de données mobiles à l'échelle mondiale devrait atteindre un taux annuel de 130 exaoctets.
- Il y aura sept milliards de nouveaux appareils sans fil sur le réseau en 2015 (notamment des modules machine-à-machine), ce qui équivaut à presque un appareil mobile par personne sur la planète.
- 1 à 2 % de tous les téléphones

Perte de contrôle – Le phénomène BYOD mobile

Dans le monde de la sécurité d'entreprise, ce qui était auparavant un univers relativement limité, avec la capacité à placer des contrôles efficaces aux points d'entrée en ligne et physiques critiques, est désormais une cible croissante, de plus en plus mobile. Le nouveau paysage dans lequel évoluent de nombreuses entreprises et organismes gouvernementaux est mobile. Les salariés, partenaires, clients et autres utilisateurs souhaitent accéder aux ressources de partout et à tout moment, en se servant des appareils mobiles les plus évolués et les plus récents qu'ils ont en main pour mener à bien leurs activités. Alors que les organisations reconnaissent les opportunités et gains de productivité pouvant découler d'un accès en tout lieu et à tout moment, elles ont du mal à assurer une prise en charge efficace.

Une des raisons fondamentales qui font que cela est si difficile est que les organisations ne possèdent plus l'ensemble des appareils qui entrent dans leurs locaux et se connectent à leurs réseaux. Les salariés emmènent leurs propres appareils (BYOD) au travail et demandent de plus en plus souvent à bénéficier du support informatique car ils veulent avoir le même accès rapide, facile et pratique aux ressources au travail, avec les mêmes appareils et outils que ceux auxquels ils sont habitués dans leur vie privée. Comme ces appareils mobiles personnels sont utilisés pour accéder aux ressources de l'entreprise et aux applications dans le cloud, ils deviennent une cible privilégiée pour les menaces de sécurité. Sur une toile de fond de quantité croissante des logiciels

malveillants mobiles, des menaces persistantes avancées et d'attaquants ultra motivés et subtils, les entreprises et organismes gouvernementaux doivent être en mesure de sécuriser l'accès mobile. Cela ne saurait être le maillon faible. L'équilibre entre

praticité et sécurité doit être maintenu en vue de garantir que la commodité octroyée par l'accès mobile ne met pas en péril les ressources et les opérations de l'entreprise.

Mais,comment les organisations protègent l'accès depuis des appareils mobiles qui ne leurs appartiennent pas ou sur lesquels elles n'ont pas de contrôle ? Elles ne peuvent pas procéder à une normalisation sur quelques, voire plusieurs, plateformes et systèmes d'exploitation pour créer un environnement cohérent ou réduire la complexité du support ; elles ne peuvent pas dire aux utilisateurs ce qu'ils doivent télécharger et ce qu'ils doivent faire avec les appareils sur leur temps propre ; et elles ne peuvent certainement pas les surveiller pour garantir qu'ils ne prêtent pas l'appareil à quelqu'un d'autre ni ne le laissent pas quelque part. Alors que les organisations et agences gouvernementales n'ont pas beaucoup de contrôle sur l'appareil, elles peuvent malgré tout contrôler l'accès qu'elles autorisent à partir de cet appareil vers les ressources de l'entreprise, leurs réseaux et leurs applications dans le cloud.

En déployant une solution complète de confirmation des identités, qui repose sur une authentification forte, les organisations peuvent avoir confiance dans l'identité de leurs utilisateurs et leurs appareils mobiles lorsqu'ils accèdent aux ressources de l'entreprise. Elles peuvent aussi gérer et contrôler cet accès. De cette façon, les organisations peuvent permettre aux utilisateurs d'accéder aux applications de l'entreprise et dans le cloud depuis leurs appareils mobiles de façon économique et plus sûre, tout en reprenant le contrôle sur leur environnement.

Une authentification forte est un élément fondamental pour sécuriser l'accès mobile

Une authentification forte, également appelée authentification avancée (AA) ou authentification à plusieurs facteurs, sert de base pour une solution efficace de confirmation de l'identité pouvant être utilisée en vue de sécuriser l'accès mobile. En demandant des facteurs supplémentaires, au-delà d'un simple mot de passe, pour valider qu'un utilisateur est bien la personne qu'il dit être, les organisations sont en mesure de déployer un niveau plus élevé de sécurité et de mieux contrôler l'accès aux ressources de l'entreprise, aux réseaux et aux applications dans le cloud. Pour pouvoir faire confiance aux appareils mobiles personnels et déployer une authentification forte, les organisations peuvent utiliser n'importe quelle combinaison de facteurs :

- Quelque chose que l'utilisateur connaît, comme un mot de passe unique ou un numéro d'identification personnel (PIN) ;
- Quelque chose que l'utilisateur possède, comme un jeton, un mot de passe à usage unique, un message SMS, ou un élément sécurisé sur un appareil mobile (comme une carte SIM, une carte à puce intégrée, un lecteur smart MicroSD, etc.) ;
- Des informations biométriques de l'utilisateur, comme ses empreintes, son iris, le modèle de sa voix ou la géométrie faciale ;
- Il peut s'agir également de paramètres réunis par le système d'identification avec une intelligence relative à la fraude ou au comportement. L'authentification peut prendre en compte les caractéristiques de l'appareil en soi, comme le type de téléphone, le navigateur, etc., l'emplacement géographique ou les caractéristiques uniques de l'utilisateur, comme les combinaisons de touche, le rythme de frappe, etc.

D'un point de vue mobile, il existe trois éléments possibles pour l'authentification. Le premier est l'authentification sur l'appareil, par exemple, quand un utilisateur allume son téléphone et entre un

code PIN pour pouvoir l'utiliser ; le deuxième est l'authentification en vue d'accéder aux ressources qui se trouvent sur l'appareil mobile ou sont accessibles via lui ; et le troisième est l'authentification auprès du portefeuille/conteneur de l'entreprise.

Le deuxième élément (l'authentification pour accéder aux ressources) correspond à l'endroit où les organisations peuvent exercer un point de contrôle. Elles peuvent s'assurer que les utilisateurs s'identifient avant d'accéder aux ressources de l'entreprise via leur téléphone personnel, tablette, etc. Une authentification forte permet aux organisations d'avoir une confiance plus élevée dans l'identité de leurs utilisateurs, puis d'accorder un accès adéquat aux VPN, bureaux virtuels, réseaux WiFi et aux applications individuelles de l'entreprise ou basées sur le cloud, tout en traitant les risques potentiels pour la sécurité qui sont associés au fait que les utilisateurs apportent leurs propres appareils dans l'environnement de l'entreprise.

Les options d'authentification répondent à différentes exigences en matière de sécurité, de commodité et de coût

Lorsque vous cherchez à protéger l'accès aux ressources et aux applications dans le cloud avec des appareils mobiles personnels, tout se résume une fois de plus à un équilibre entre coût, commodité et sécurité. Il existe plusieurs approches qui ajoutent divers niveaux de sécurité et introduisent divers niveaux de complexité. Les organisations doivent prendre en compte les besoins des utilisateurs, ainsi que les coûts, aussi bien en termes d'investissements en capital que de frais opérationnels continus, pour l'organisation.

Une option peut consister en ce que certains utilisateurs ou applications requièrent des niveaux supplémentaires de sécurité et différents niveaux d'accès. De ce fait, les organisations peuvent en arriver à déployer diverses méthodes d'identification pour contrôler l'accès de façon appropriée. Lorsque ces méthodes sont combinées, une organisation peut adopter une approche à plusieurs couches de l'identification mobile qui répond à ses critères en termes de sécurité et de coûts, ainsi qu'aux attentes de ses utilisateurs lorsqu'ils se servent de leur propre appareil mobile. Voici quelques-unes des options d'identification que l'organisation peut envisager pour protéger l'accès aux ressources de l'entreprise avec des appareils personnels :

- **Mots de passe statiques :** Ils ne sont tout simplement pas suffisants. Ils sont vulnérables aux espions de clavier, attaques de phishing, etc., et n'assurent aucune protection contre les menaces internes.

- **Jeton matériel :** Un périphérique qui peut être utilisé pour une authentification à facteurs multiples. Les jetons matériels offrent une sécurité forte. Toutefois il incombe à l'utilisateur de les transporter et de ne pas les oublier, ce qui influe négativement sur son expérience d'utilisation. Lorsque l'utilisateur doit s'identifier, il regarde le jeton et insère le mot de passe unique qu'il a généré pour obtenir un accès (si l'appareil a un lecteur, l'utilisateur peut aussi placer le jeton contre le lecteur pour s'identifier). Les jetons peuvent accroître les coûts généraux pour une organisation, car ils doivent être achetés, envoyés, gérés et maintenus. Notez que ces jetons peuvent être fournis sous la forme d'une clé USB, ce que certains téléphones ne prennent pas en charge.

- **Jeton logiciel mobile :** Fourni en tant qu'application autonome ou intégré dans une application que quelqu'un développe, le jeton logiciel est téléchargé par l'utilisateur pour faire office de mot de passe à usage unique dans le cas d'une authentification à facteurs multiples. Cela peut ne pas être aussi fort que lorsque les clés du mot de passe à usage unique sont générées sur une puce dédiée et certifiée inviolable, mais de nombreux jetons

de ce type bénéficient d'une technologie spéciale anti-clonage intégrée pour prévenir la contrefaçon ou le clonage du jeton sur un autre appareil. Lorsqu'ils doivent s'identifier pour accéder à une ressource de l'entreprise ou une application dans le cloud, les utilisateurs cliquent simplement sur le jeton logiciel mobile (app), entrent un code pin et utilisent le mot de passe à usage unique valide pendant environ une minute pour obtenir un accès. Cela ne requiert aucun matériel, ce qui le rend très facile à déployer et à gérer, et permet à l'utilisateur de l'intégrer sans peine dans son flux de travail.

- **Message SMS** : Agit comme un mot de passe à usage unique envoyé par SMS. Identique à la délivrance d'un mot de passe à usage unique via un jeton logiciel mobile, mais au lieu de cliquer sur une application pour obtenir le mot de passe à usage unique, l'utilisateur fait une demande et reçoit un mot de passe à usage unique par SMS, puis doit ensuite le copier et le coller dans l'application. C'est donc légèrement moins pratique pour l'utilisateur qu'un jeton logiciel. C'est aussi moins sûr car le SMS peut être intercepté et n'arrive pas toujours à destination. Il existe aussi un coût associé à l'envoi de SMS.

- **Jetons de sécurité basé sur des éléments sécurisés :** Mécanisme de sécurité intégré à l'appareil mobile qui permet aux utilisateurs de s'appuyer sur des moyens d'identification forts. Notez que les plateformes mobiles, qui ont divers niveaux de maturité, doivent être en mesure d'avoir l'élément sécurisé déjà intégré ou un endroit permettant de conserver la carte à puce ou microSD, de sorte qu'elle puisse être utilisée pour différents usages, comme l'authentification, le chiffrement, le déchiffrement, la signature d'e-mail et la fourniture d'un accès physique sécurisé et d'un accès aux applications dans le cloud. Cette solution offre le niveau de sécurité le plus élevé ; elle est également pratique pour l'utilisateur car il peut faire tout ce dont il a besoin de façon sécurisée. Elle peut être coûteuse à l'achat, mais il existe sur le marché des solutions innovantes qui simplifient le déploiement et la gestion des éléments sécurisés et des moyens d'identification qu'elles abritent. À ce jour, elle est principalement utilisée par des organismes gouvernementaux et industries régulées ayant besoin d'adhérer aux normes et réglementations.

BYOD – Options d'authentification fortes

Option	Description	Sécurité	Complexité	Coût	Commodité
Mot de passe	Mot de passe simple	Faible	Faible	Faible	Élevée
Jeton matériel	Mot de passe à usage unique développé en matériel	Élevée	Élevée	Élevée	Faible
Jeton logiciel mobile	Agit comme un mot de passe à usage unique fourni une application	Moyenne	Faible	Faible	Moyenne
Message SMS	Agit comme un mot de passe à usage unique fourni un SMS	Faible/Moyenne	Faible	Faible	Moyenne
Élément sécurisé	SIM, carte à puce intégrée, ou Smart	Élevée	Élevée	Élevée	Élevée

	microSD installé sur le téléphone				

Comment fonctionne l'authentification vers les applications dans le cloud
L'organisation peut utiliser les solutions ActivID® de HID Global pour déployer diverses méthodes d'authentification, tout en maintenant une expérience utilisateur simple et en limitant les risques pour la sécurité associés au fait d'utiliser son appareil personnel (BYOD). Par exemple, un utilisateur se rend sur l'app store, télécharge l'application de jeton logiciel (ou l'organisation peut l'imposer) pour commencer le processus d'enregistrement auprès d'ActivID.

L'administrateur de l'organisation envoie ensuite un e-mail avec plusieurs codes que l'utilisateur saisit afin de recevoir la confirmation qu'il a bien été lié à cet appareil dans le système. L'utilisateur peut alors s'identifier en vue de sécuriser l'accès à partir de cet appareil vers le réseau de l'entreprise et/ou les applications dans le cloud.

Par exemple, le dispositif ActivID utilisera le langage de balisage d'assertion de sécurité (SAML) pour travailler avec Salesforce.com ; lorsque l'utilisateur voudra accéder à Salesforce.com, il sera automatiquement redirigé vers le dispositif. Il devra alors utiliser son moyen d'identification pour s'authentifier et obtenir un accès. Ce ticket SAML peut être utilisé par d'autres applications dans le cloud ou applications de l'entreprise pour accorder un

Les exigences pour une solution efficace d'identification pour un accès mobile sécurisé (BYOD)

Le paysage mobile évolue tous les jours ; de nouveaux appareils font leur apparition et les plateformes mobiles évoluent à un tel rythme qu'il est quasiment impossible pour les organisations de suivre. Les utilisateurs sont prompts à adopter le dernier appareil et à l'amener dans l'environnement dans l'entreprise, en demandant l'accès aux ressources. Pour permettre efficacement l'accès via des appareils mobiles personnels, sans confronter l'organisation à des risques ou coûts inutiles, les solutions doivent fournir :

- **Réduction des risques** – Rien ne va éliminer le danger que présentent les menaces en constante évolution et constante progression. Ce qu'il faut, c'est un moyen de minimiser l'exposition de l'organisation aux risques introduits par l'accès mobile. La solution doit offrir :

- **Authentification forte** – deux facteurs ou plus, en vue d'accroître la confiance que les organisations ont dans l'identité de leurs utilisateurs et leur capacité à octroyer un accès adéquat à partir des appareils mobiles.

- **Différents niveaux d'accès** – d'après les risques associés aux différents types d'utilisateurs et la sensibilité des ressources de l'entreprise et des applications dans le cloud accessibles via cet appareil mobile.

- **Contrôle de la plateforme** – pour répondre aux plateformes mobiles disponibles que les organisations peuvent avoir dans leur environnement. Les organisations devraient être en mesure d'imposer les plateformes et les versions spécifiques de chaque plateforme autorisées à accéder à leurs réseaux et applications. Par exemple, une organisation peut être au courant qu'une version spécifique d'un système d'exploitation mobile est vulnérable aux attaques et peut décider de ne pas autoriser les dispositifs l'utilisant d'accéder au réseau/aux ressources.

- **Réponse rapide et ciblée** – En cas d'incident de sécurité, les organisations doivent avoir les outils et les moyens permettant d'y répondre facilement et rapidement de façon ciblée sans que les utilisateurs non affectés par l'incident ne soient impactés. Par exemple, elles doivent être en mesure d'empêcher l'accès à partir d'un dispositif particulier ou d'une version spécifique d'applications/de logiciel présentant un risque élevé, peut-être en raison d'une vulnérabilité spécifique.

- **Maniabilité** – la solution doit être facile à installer et à utiliser, ans ajouter de complexité ou de coûts inutiles. Idéalement, elle devrait permettre aux organisations d'avoir une vue consolidée qui simplifie l'émission des moyens d'identification et la gestion continue pour assurer une position cohérente en matière de sécurité. Par exemple, il devrait être aisé d'identifier et de

révoquer des moyens d'identification pour que l'organisation ne laisse pas actif le moyen d'identification d'un salarié qui ne fait plus partie du personnel.

Polyvalence – La solution doit être polyvalente et modulable, de sorte que les organisations puissent satisfaire leurs différentes exigences. La solution doit prendre en charge :

- **Multiples méthodes d'authentification** – Pour équilibrer les exigences d'une organisation en matière de coûts et de sécurité, la solution doit être suffisamment flexible pour prendre en charge différentes méthodes d'authentification pour différents utilisateurs, ressources et applications dans le cloud.

- **Technologie basée sur des normes de référence** – Dans le paysage mobile à évolution rapide actuel, les organisations veulent une solution proposée par un fournisseur ayant une bonne expérience de recherche innovante de solutions à des problèmes difficiles. La solution doit adhérer aux normes, de manière que les organisations puissent déployer les technologies au fur et à mesure de leur disponibilité, sans devoir compter sur le calendrier d'un fournisseur quel qu'il soit.

- **Vaste prise en charge de plateforme** – Avec BYOD, le champ libre est vaste. Les utilisateurs peuvent utiliser toute sorte d'appareils, avec différents systèmes d'exploitation et différentes versions de ces systèmes d'exploitation, proposés par divers fournisseurs. Ce dont les organisations ont besoin, c'est une solution pouvant être utilisée dans l'ensemble des appareils mobiles de façon à garantir que les contrôles d'accès sont appliqués de façon uniforme et simple à gérer.

- **Praticité pour les utilisateurs** – la solution ne devrait pas interrompre les flux de travail ou provoquer des retards indus pour l'entreprise et les utilisateurs d'applications dans le cloud doivent pouvoir mener leurs activités à bien.

Approche de HID Global concernant l'authentification mobile – Options complètes, flexibles et sécurisées

Avec HID Global, les organisations peuvent établir la confiance dans les identités de leurs utilisateurs lorsqu'ils accèdent à des ressources à partir de leurs appareils mobiles, puis gérer cet accès en vue de protéger l'entreprise et les applications dans le cloud. HID Global, leader mondial dans le domaine des solutions d'identité sécurisée, fournit depuis longtemps des solutions de confirmation d'identité complètes et innovantes qui répondent aux exigences des organisations en matière de sécurité et de coûts, tout en répondant également aux attentes de leurs utilisateurs. En fonction des besoins de l'organisation, la solution offerte peut compter un ou plusieurs produits combinés du portefeuille Identity Assurance de HID Global. HID Global offre tout un ensemble de produits d'authentification et de gestion des moyens d'identification et a émis plus de 20 millions de moyens d'identification dans le monde. Le portefeuille inclut :

La polyvalence d'ActivID de HID Global en bref

- **Prise en charge des périphériques** : smartphones, tablettes, ordinateurs portables et autres périphériques

- **Méthodes d'identification :** Jetons matériels avec mot de passe à usage unique et jetons logiciels, cartes à puce (PKI), identifiants par périphérique, authentification adaptative, mécanismes de protection contre la fraude, et SMS hors bande, ou mécanismes de mot de passe à usage unique par e-mail pour une authentification au niveau de la transaction

- **Jetons logiciels mobiles et kit de développement logiciel de HID Global (jetons ActivID® de HID Global)** – les jetons logiciels peuvent être distribués sur le réseau et rapidement téléchargés par les utilisateurs (ou téléchargés depuis un app store). Les utilisateurs peuvent simplement générer un mot de passe à usage unique quand ils veulent se connecter via leur appareil mobile aux ressources de l'entreprise. Les jetons logiciels mobiles de HID Global sont disponibles sur les principaux systèmes d'exploitation pour appareils mobiles notamment RIM

BlackBerry®, Apple® iOS (pour iPhone® et iPad), Google Android, Windows Mobile et bien d'autres périphériques fonctionnant sous Java 2 Platform, Micro Edition (J2ME). Ils sont fournis avec la possibilité d'un remplacement à vie et un contrat de maintenance. Les organisations peuvent aussi utiliser kit de développement logiciel du jeton logiciel mobile de HID Global, qui peut être intégré directement dans l'application mobile, par exemple une application bancaire mobiles offerte par une banque au détail.

- **ActivClient™ Mobile de HID Global** – Intergiciel qui utilise un élément sécurisé local sur le téléphone pouvant être une carte Smart microSD, une carte à puce intégrée, ou même la carte SIM ou une carte à puce existante (par exemple, cartes PIV, PIV-I, CIV), insérée dans le téléphone, via un lecteur relié (par exemple sous la forme d'un étui), pour fournir les niveaux d'assurance les plus élevés pour les services de sécurité, depuis l'authentification forte et la non-répudiation jusqu'à la signature numérique et les services de chiffrement. Prend en charge les applets certifiés FIPS de HID Global qui fournissent des composants fiables de niveau gouvernemental d'une carte de vérification d'identité personnelle “sur le téléphone”.

  Par exemple, les utilisateurs peuvent avoir des e-mails sécurisés et signés numériquement sur leur téléphone. ActivClient agit comme un intergiciel, permettant à l'organisation d'exploiter la fonctionnalité de sécurité sur l'élément sécurisé. Il assure l'interface avec les applets de HID Global sur l'élément sécurisé en vue de tirer le meilleur profit des moyens d'identification à clé publique-privée, facilitant ainsi l'utilisation de l'infrastructure de clé publique (PKI) pour la messagerie électronique sécurisée. Comme le mécanisme se trouve dans le téléphone, il n'est pas nécessaire de lier ou d'appairer un lecteur de cartes à puce au dispositif, ce qui le rend bien plus pratique pour l'utilisateur et bien moins compliqué pour l'organisation.

- **Alliance stratégique avec Good Technology** – offre un ensemble de nouvelles solutions de gestion, de messagerie et de collaboration d'entreprise mobile, de niveau gouvernemental pour les plateformes iOS et Android. Les solutions réunissent les capacités de sécurité existantes, de niveau gouvernemental, de Good for Enterprise™ et Good for Government™ avec la technologie d'authentification forte de l'intergiciel ActivClient® Mobile de HID Global. Elles permettent aux salariés des industries réglementées et des gouvernements, ainsi qu'aux entreprises qui les prennent en charge, d'accéder à des applications pertinentes en se servant de leur appareil mobile, tout en maintenant les niveaux de sécurité nécessaire requis par l'organisation. La solution aide à compartimenter l'accès aux ressources à partir du téléphone mobile, en particulier pour les scénarios BOYD, en vue d'atténuer les risques.

ActivID CMS en un bref

- **Dispositifs d'authentification** : des cartes à puce et jetons USB aux éléments sécurisés sur les téléphones mobiles
- **Données** : mots de passe statiques, biométrie et données démographiques
- **Applets :** Applications de mots de passe à usage unique et applets de vérification d'identité personnelle

- **Système de gestion des informations d'identification ActivID de HID Global** – fournit une solution complète et flexible pour permettre aux organisations de gérer facilement les besoins d'émission et de gestion des déploiements d'authentification réussis. Les organisations peuvent émettre et gérer des éléments sécurisés, cartes à puce, jetons USB intelligents, etc. pouvant être utilisés pour l'identification auprès d'applications depuis des appareils mobiles. Le système ActivID fournit des capacités de gestion du cycle de vie sans fil pour permettre le verrouillage de l'élément sécurisé (ainsi que de l'ensemble des certificats et clés liés) quand le téléphone est sur le terrain ; les capacités en libre service permettent à un utilisateur de déverrouiller un code PIN verrouillé ou de recevoir un nouveau moyen d'identification (par exemple, un nouveau certificat PKI et une clé privée liée) quand il est sur site, sans devoir retourner à un bureau de service.

Il offre des fonctionnalités d'audit complète et inviolables qui enregistrent toutes les activités d'événement à des fins de reporting, avec des capacités de mise à jour post-émission sécurisées, brevetées et uniques pour aider à maintenir la solution d'authentification de l'organisation en vigueur. L'administration du libre service et de l'assistance technique basée sur le Web réduit les coûts d'exploitation associés à la gestion continue et à la maintenance de la solution.

- **Le dispositif d'authentification ActivID de HID Global** – assure une authentification polyvalente forte, comprenant une authentification par SMS hors bande, pour les utilisateurs qui accèdent à un vaste éventail d'applications, comme l'accès à distance au VPN, les bureaux virtuels, les services de terminaux, et les clouds privés et publics. Grâce à un dispositif simple, HID Global prend en charge une multitude de méthodes d'authentification pour protéger les données de l'organisation, son réseau et ses actifs en termes de réputation.

  ActivID permet à l'organisation d'adapter les méthodes d'authentification aux besoins de groupes spécifiques d'utilisateurs, fournissant à chacun le bon équilibre de sécurité, coût et commodité pour répondre aux objectifs commerciaux. Les modèles et politiques faciles à définir permettent aux organisations d'être aussi spécifiques qu'elles le veulent, limitant l'accès à des appareils particuliers dans une certaine zone ou prenant en compte le rôle de l'utilisateur (par exemple s'il s'agit d'un PDG ou directeur marketing) et déterminant le moyen d'identification qu'il convient de fournir et la manière de gérer l'accès.

  HID Global augmente la productivité en authentifiant en toute sécurité les utilisateurs à distance via leur smartphone, navigateur ou ordinateur préféré, via divers périphériques et méthodes d'authentification. Le dispositif ActivID prend en charge le plus vaste choix de méthodes d'authentification, depuis les mots de passe forts jusqu'à l'authentification basée sur des certificats, en passant par les jetons matériels à deux facteurs basés sur des normes OATH (Authentification ouverte), jetons logiciels, et possibilités de mots de passe à usage unique hors bande par SMS. Le dispositif ActivID réduit les coûts grâce à des jetons faciles à installer et d'utilisation simple qui dure jusqu'à huit ans, et une intégration simple dans l'infrastructure réseau existante.

  Le service de détection des menaces avancé ActivID de HID Global est un service unique d'identification des appareils basé sur le cloud et un service mondial de détection des fraudes qui permet aux organisations d'ajouter efficacement des mesures de lutte contre la fraude à leurs systèmes d'authentification. Le profilage en temps réel des périphériques et les services de localisation mobiles peuvent être utilisés pour fournir un facteur de confiance supplémentaire. Avec plus de 300 clients directs, 1,2 million de nouveaux appareils et 1,3 million de transactions profilées chaque jour, les organisations bénéficient d'une bonne visibilité sur les changements importants qui se produisent au niveau des menaces de façon à combattre les cyber criminels et prévenir la fraude en ligne. Le service de détection des menaces ActivID leur donne la possibilité de détecter et de bloquer l'accès depuis des ordinateurs compromis ou frauduleux ; d'identifier instantanément les mots de passe volés, de bloquer des comptes et d'informer les utilisateurs légitimes de la nécessité de changer leur mot de passe ; ainsi que d'empêcher tout accès frauduleux et autre risque potentiellement à haut risque.

Avec HID Global, les organisations peuvent bénéficier des avantages de l'accès mobile sécurisé, notamment l'accès à partir d'appareils personnels

Fort d'une longue expérience dans le domaine de l'identification et des moyens d'authentification, HID Global est en mesure de fournir aux organisations toutes les pièces dont elles ont besoin pour sécuriser l'accès mobile, depuis le système de gestion des moyens d'identification et la plateforme de validation jusqu'aux jetons logiciels et aux puces (et même sur le téléphone ou les lecteurs, si nécessaire). HID Global protège les données bancaires en ligne et l'accès aux applications sensibles d'entreprise et dans le cloud de millions d'utilisateurs, dans des institutions financières, organismes de soins de santé, entreprises et agences gouvernementales. HID global est le partenaire de choix pour la gamme complète des besoins des clients dans le domaine de la confirmations d'identité et de l'authentification forte. L'entreprise applique cette expérience au paysage mobile embryonnaire en constante évolution pour aider les organisations à adopter en douceur la mobilité. Avec HID Global, les entreprises peuvent :

- **Réduire les risques** – permettre aux utilisateurs de se connecter en toute sécurité avec leurs appareils mobiles, via une authentification forte à facteurs multiples qui empêche les violations et protège les ressources de l'entreprise et les applications dans le cloud. Répondez aux exigences d'utilisation d'une authentification forte pour l'accès mobile et assurez-vous que ce n'est pas le maillon faible dans la position de l'organisation devant la sécurité.

- **Réduire les coûts** – grâce à des technologies d'authentification polyvalentes et multi-couches, les organisations ont ce qu'il leur faut pour sécuriser l'accès par smartphone, iPad, ordinateur portable et autre accès mobile aux VPN, portails Web et applications dans le cloud. La gestion centralisée simplifie les processus, réduite la paperasse et rationalise les opérations générales associées à la solution de confirmation d'identité de l'organisation. Le vaste éventail d'options permet aux organisations de choisir la meilleure solution pour leurs différents besoins, éliminant par là même les coûts associés à une solution unique. Les organisations peuvent choisir le niveau de sécurité dont elles ont besoin pour leurs différents utilisateurs, ressources d'entreprise et applications, et adapter facilement leurs déploiements au fur et à mesure que leurs besoins changent.

- **Améliorer le contrôle** – employez une solution d'authentification entièrement interopérable basée sur des normes OATH (Authentification ouverte) pour vous assurer que les utilisateurs peuvent accéder en toute sécurité à ce dont ils ont besoin pour mener leurs activités à bien en se servant de leurs appareils mobiles. Les politiques de sécurité et processus commerciaux faciles à définir permettent aux organisations d'émettre et de gérer en toute simplicité des moyens d'identification et de fournir différents niveaux d'authentification pour différentes ressources et applications dans le cloud afin de répondre aux exigences de l'entreprise en matière de coûts, de sécurité et de complexité.

- **Offrir la commodité aux utilisateurs** – s'assurer que les utilisateurs ont les accès dont ils ont besoin, quand ils en ont besoin et où qu'ils se trouvent, de façon à optimiser la productivité. Les solutions faciles à utiliser renforcent la sécurité de façon transparente, sans interruptions inutiles du flux de travail.

Résumé

Comme les smartphones sont de plus en plus intelligents et que les tablettes et autres dispositifs sont utilisés pour faire de plus en plus de choses, ils vont être de plus en plus la cible des attaquants. Les smartphones accèdent non seulement aux e-mails, mais aussi à un volume croissant de données et systèmes d'entreprise sensibles, aussi bien directement que via des applications dans le cloud. Il est important de réduire l'exposition à ces nouvelles menaces et dangers, tout en permettant aux utilisateurs de se servir de leurs appareils mobiles pour mener leurs affaires et maintenir la conformité avec les réglementations en vigueur. Les organisations ont

besoin de mesures de sécurité capables de fonctionner avec un large éventail de types d'appareils (plateformes et systèmes d'exploitation) et d'implémenter la sécurité et la praticité que requièrent les différentes applications.

HID Global applique une longue expérience en matière de confirmation d'identité et d'authentification sur le marché en constante évolution des appareils mobiles de façon à fournir des solutions qui permettent aux organisations de sécuriser efficacement l'accès mobile aux ressources des entreprises, leurs réseaux et leurs applications dans le cloud. Grâce à un portefeuille vaste et complet qui inclut tout, depuis des solutions non matérielles sécurisées (avec des jetons logiciels et une capacité de détection des fraudes) aux solutions à éléments sécurisés LoA4, les organisations peuvent atteindre le niveau de confirmation d'identité dont elles ont besoin en faisant appel à un fournisseur fiable unique. Les organisations ont la capacité d'appliquer la sécurité dont elles ont besoin pour leur accès mobile, d'une manière qui réduit les risques et les coûts, tout en assurant la commodité pour leurs utilisateurs. Avec HID Global, les organisations peuvent reprendre le contrôle sur leurs environnements et prendre en charge l'accès mobile de manière pratique et sécurisée en vue de pouvoir saisir les opportunités et d'encourager la productivité.

2014-03-28-MobileAuthentication-wp-fr PLT-02014